DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**Addendum**") forms part of the engagement letter, Master Services Agreement, Master Software as a Service Agreement, Subscription License Agreement, or any other written agreement (including any Statement(s) of Work) that incorporates this Addendum by reference, including by hyperlink, as applicable, between Client and Crowe (collectively, the "**Agreement**"), with Client and Crowe each being a "**Party**" and together the "**Parties**".

In order to provide the Services set forth in the Agreement, Client may disclose Client Personal Data regarding its accounts, personnel, or customers to Crowe. This Addendum applies solely to the extent Crowe processes Client Personal Data in connection with the Services. The Parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Agreement, incorporated by reference therein, and references in this Addendum to the Agreement are to the Agreement as amended by, and including, this Addendum.

1. Definitions. Capitalized terms in this Addendum have the meaning set forth below or elsewhere in this Addendum. Other capitalized terms have the meaning set forth in the Agreement or as defined in Data Privacy Laws. The terms "**Business**", "**Controller**", "**Data Subject**", "**Personal Data**", "**Personal Information**", "**Personal Data Breach**", "**Process**", "**Processor**", "**Service Provider**" and other like terms have the same meanings set forth in the Data Privacy Laws.

"**Client Personal Data**" means any Personal Data Processed by Crowe on behalf of Client in connection with the Services.

"**Cross-Context Behavioral Advertising**" means the targeted advertising to an individual based on the individual's Personal Information obtained from the individual's activity across businesses, distinctly branded websites, applications, or services.

"**Data Privacy Laws**" means as directly applicable to Crowe's provision of the Services: (i) Regulation (EU) 2016/679 ("**GDPR**") together with applicable legislation implementing or supplementing the same or otherwise relating to the processing of Personal Data of natural persons, (ii) to the extent not included in sub-clause (i), the Data Protection Act 2018 of the United Kingdom, as amended from time to time, and including any substantially similar legislation that replaces the DPA 2018 ("**UK Data Privacy Laws**"), (iii) the national legislation of the Swiss Confederation on the protection of Data Subjects with regard to the processing of Personal Data and on the free movement of such data, as amended from time to time, and other data protection or privacy legislation in force from time to time in the Swiss Confederation, (iv) the California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act and including its implementing regulations ("CCPA"), the Colorado Privacy Act, the Connecticut Data Privacy Act, the Delaware Personal Data Privacy Act, the Montana Consumer Data Protection Act, the Texas Data Privacy and Security Act, the Utah Consumer Privacy Act, or the Virginia Consumer Data Protection Act, in each case as amended and to the extent effective and including its respective implementing regulations, and any other applicable state or federal laws or regulations concerning privacy.

"**EU-US Data Privacy Framework**" or "**DPF**" means the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S. Data Privacy framework developed by the U.S. Department of Commerce and the European Commissions, UK Government, and Swiss Federal Administration to provide U.S. organizations with reliable mechanisms for personal data transfers to the United States from the European Union, United Kingdom, and Switzerland while ensuring data protection that is consistent with EU, UK, and Swiss law. More information is available at https://www.dataprivacyframework.gov/s/ and evidence of Crowe's DPF Certification is set forth on the DPF's website at https://www.dataprivacyframework.gov/s/participant-search/participant-detail?id=a2zt00000008hFhAAI&status=Active.

"**Restricted Personal Data**" means Personal Data consisting of protected health information, financial account numbers, Social Security or other government-issued identification numbers, or other data that, if disclosed without authorization, would trigger notification requirements under applicable law.

"**SCCs**" means the Standard Contractual Clauses set out in the annex to the Commission Implementing Decision (EU) 2021/914, available at https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en and as configured in **Exhibit A**.

"**Services**" means the services to be performed by Crowe for the Client pursuant to the Agreement.

"**UK IDTA**" means the United Kingdom International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the United Kingdom Information Commissioner on March 21, 2022, and with its tables completed as in **Exhibit B**.

2. Cross-Border Transfers of EEA/Swiss and UK Personal Data.

a. To the extent Crowe processes Personal Data originating from the European Economic Area ("EEA"), Switzerland, or the United Kingdom ("UK"), Crowe shall comply with the applicable principles under the EU-U.S. Data Privacy Framework, including its UK and Swiss extensions, as described in Section 3 below. Crowe certifies that it is self-certified under these frameworks for the duration of the Agreement.

b. If, during the term of the Agreement, any of these frameworks or Crowe's certification thereunder is invalidated or otherwise no longer deemed an adequate safeguard for cross-border transfers under Article 45 of the GDPR or equivalent UK or Swiss provisions, the Parties agree that such transfers shall instead be subject to the SCCs and/or the UK IDTA, as applicable. In such event, the SCCs and UK IDTA shall be deemed automatically incorporated into the Agreement without further action by the Parties, as described in Section 5 below. If the DPF becomes invalid or unavailable, and SCCs or UK IDTA are also inapplicable, the Parties will evaluate and agree in good faith on an alternative valid transfer mechanism (e.g., binding corporate rules or appropriate derogations under Article 49 GDPR).

3. Data Privacy Framework. Crowe represents that it has self-certified to, and will maintain its certification under, the EU-U.S. Data Privacy Framework, including the UK Extension and Swiss-U.S. Framework, for the duration of the Agreement. Crowe agrees to maintain a level of protection for Personal Data originating from the EEA, UK, or Switzerland that is at least equivalent to the protections required under the applicable frameworks. Crowe shall comply with the relevant principles of the frameworks for as long as it continues to process such data in connection with the Agreement. Crowe's certification status may be verified at https://www.dataprivacyframework.gov/s/.

4. Roles of the Parties. The Parties acknowledge and agree that, with respect to the Processing of Client Personal Data, and as further described in Schedule 1, each of the Client and Crowe shall act either as a Controller or a Processor, as determined by the nature of the Services and in accordance with applicable Data Privacy Laws. Where Crowe is engaged as a Service Provider, its role shall be interpreted based on the context and applicable legal definitions.

a. The Parties expressly agree that Client shall be solely responsible for ensuring timely communications to Client's affiliates or the relevant Controller(s) who receive the Services, insofar as such communications may be required or useful in light of applicable Data Privacy Laws to enable Client's affiliates or the relevant Controller(s) or Business(es) to comply with such Data Privacy Laws.

b. The Parties acknowledge and agree that no monetary or other valuable consideration is being provided by Crowe to Client in exchange for Client Personal Data, and Client Personal Data is not being provided for purposes of Cross-Context Behavioral Advertising, and therefore Client is not "selling" or "sharing" Client Personal Data with Crowe, as those terms are defined under the CCPA.

5. Nature of the Processing. Crowe processes Personal Data or Personal Information: (a) performing the Services and its obligations under the Agreement, (b) as otherwise set forth in the Agreement, (c) to detect security incidents and protect against fraud or illegal activity, (d) to enhance and develop Crowe's products and services in an aggregated or de-identified form, or as otherwise permitted by applicable law or the Agreement, and (e) as necessary to comply with applicable law or professional standards.

6. Data Processing Terms.

a. **General Client Obligations.** Client warrants (i) that it has the authority to provide Client Personal Data to Crowe in connection with the Services, (ii) that it has processed and provided Client Personal Data to Crowe in accordance with applicable Data Privacy Laws, and (iii) that it will limit the Client Personal Data provided to Crowe to Client Personal Data necessary to perform the Services. As between the Parties, Client shall be solely responsible for compliance with applicable Data Privacy Laws regarding the collection of and transfer to Crowe of Client Personal Data, including providing any notices to Data Subjects and obtaining any required consents from such Data Subjects. Client hereby authorizes Crowe to collect, process, retain, disclose, and destroy Client Personal Data as reasonably necessary for the provision of the Services.

b. **General Crowe Obligations.** Crowe shall:

(i) process the Client Personal Data solely pursuant to the documented instructions of Client, for the purposes of providing the Services, including for internal review and improvement of the Services as reasonably necessary for the provision of Services, as otherwise set forth in the Agreement, to detect security incidents and protect against fraud or illegal activity, to enhance and develop our products and services, including through machine learning and other similar methods and as necessary to comply with applicable law or professional standards or as otherwise necessary to perform its obligations under the Agreement or required by applicable law;

(ii) not retain, use or disclose Personal Data for any purpose other than as necessary to perform the Services, to comply with applicable law or professional obligations, or as otherwise set forth in the Agreement;

(iii) not combine Client Personal Data with personal data received from other clients or collected independently by Crowe, except as necessary for permissible business purposes under applicable Data Privacy Laws, or as otherwise expressly permitted in the Agreement;

(iv) to the extent permitted by applicable law, not disclose any Client Personal Data, except to Client and Crowe's personnel or use as necessary or allowed under Data Privacy Laws;

(v) require that persons authorized to Process the Client Personal Data are subject to confidentiality obligations or are otherwise under an appropriate statutory or professional obligation of confidentiality;

(vi) implement and maintain the technical and organizational measures set forth at https://www.crowe.com/iss, which the parties have mutually agreed pursuant to Article 32 of the GDPR or other Data Privacy Laws, having regard to the assessment of the appropriate level of security for Client Personal Data and the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access or damage to such Personal Data;

(vii) notify Client without undue delay, however, in no event longer than three (3) business days, of any Personal Data Breach involving Client Personal Data, upon Crowe's becoming aware of a Personal Data Breach involving Client Personal Data, such notice will include all information reasonably required to enable Client to comply with its obligations under Data Privacy Laws, to the extent known to Crowe at the time; and

(viii) cease Processing the Client Personal Data upon the termination or expiration of the Agreement. Upon Client's request, Crowe will either return or delete all copies of the Client Personal Data Processed by Crowe. Notwithstanding the foregoing or anything to the contrary contained herein, Crowe may retain Personal Data as set forth in Section 6(f).

c. **Obligations as a Service Provider.** Crowe is a Service Provider, as defined by the CCPA, and shall comply with the CCPA as directly and to the extent applicable in Crowe's performance of the Services. With respect to Client Personal Data for California consumers, the Parties agree that:

(i) Crowe will not sell or share Client Personal Data it collects on behalf of Client under the Agreement to the extent prohibited by the CCPA;

(ii) Client is disclosing Client Personal Data to Crowe for the purpose(s) identified herein;

(iii) Crowe may not retain, use or disclose Client Personal Data it collects on behalf of Client under the Agreement: (1) for any purpose other than the purpose(s) identified herein or as otherwise permitted by the CCPA; (2) for any commercial purpose other than the purpose(s) identified herein or as expressly permitted by the CCPA; or (3) outside the direct business relationship between Crowe and the business, except as expressly permitted by the CCPA;

(iv) To the extent expressly required by the CCPA, Client may take reasonable and appropriate steps necessary to ensure that Crowe uses the Client Personal Data it collected under the Agreement in a manner consistent with Crowe's obligations under the CCPA;

(v) Crowe will notify the Client if Crowe makes a determination that it can no longer meet its obligations under the CCPA, and upon such notice Client may take reasonable and appropriate steps to stop and remediate Crowe's unauthorized use of Client Personal Data;

(vi) Crowe shall provide reasonable assistance described in Section 8 (Assistance) of this Addendum to Client as required for Client to comply with consumer requests.

d. **Assistance with Compliance and Data Subject Requests.** To the extent required by Data Privacy Laws, Crowe shall:

(i) to the extent legally permissible, promptly notify Client, if applicable, of any communication from a Data Subject or a supervisory authority relating to the Processing of Client Personal Data, or any other communication regarding an obligation under the Data Privacy Laws in respect of the Client Personal Data and, taking into account the nature of the Processing, assist Client, if applicable, by appropriate technical and organizational measures, insofar as this is practical, for the fulfillment of Client's obligation to respond to requests for exercising the Data Subject's rights laid down in Chapter III GDPR. Client agrees to reimburse Crowe for reasonable professional time and out-of-pocket expenses incurred in connection with such assistance, unless prohibited by applicable law;

(ii) assist Client with its obligations pursuant to Articles 32 to 36 of the GDPR taking into account the nature of the Processing and information available to Crowe. Client agrees to pay Crowe for its professional time and out-of-pocket expenses incurred by Crowe in connection with any assistance provided with regards to Articles 35 and 36 of the GDPR.

e. **Restricted Personal Data.** In the event Client provides Crowe access to Restricted Personal Data, Client will consult with Crowe on appropriate measures (consistent with legal requirements and professional standards applicable to Crowe) to protect the Restricted Personal Data, such as: deleting or masking unnecessary information before making it available to Crowe, using encryption when transferring it to Crowe, or providing it to Crowe only during on-site review on Client's site or through Virtual Desktop Infrastructure (VDI). Client will provide Crowe with Restricted Personal Data only in accordance with mutually agreed protective measures.

f. **Deletion of Client Personal Data.** As appropriate, Crowe shall promptly delete or procure the deletion of Client Personal Data, after the cessation of any Services involving the processing of Client Personal Data, or otherwise aggregate or de-identify the Client Personal Data in such a way as to reasonably prevent reidentification. Notwithstanding the foregoing, Crowe may retain a copy of the Client Personal Data on any automatic backup disaster recovery system or server provided that non-deleted data will be held securely and securely deleted in accordance with Crowe backup retention policies or as permitted by applicable law or professional standards, provided that such Client Personal Data remain subject to the terms of the Agreement.

g. **US Federal Rules.** The Safeguards set forth in Schedule 2 will meet the objectives of the Interagency Guidelines Establishing Information Security Standards, adopted by the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation, as they currently exist, or as they may be amended from time to time.

h. **Sub-Processors.** Client hereby expressly and generally authorizes Crowe to engage other Processor(s) or Service Providers to Process the Client Personal Data ("**Sub-Processor**") as set forth in Schedule 3, subject to Crowe's including data protection terms in its contract with each Sub-Processor which are substantially similar to those set out in this Addendum; and remains responsible to the Client for any failure by each Sub-Processor to fulfill its obligations in relation to the Processing of the Client Personal Data. Crowe shall notify Client of any changes to Sub-Processors by updating the hyperlink in Schedule 3. If Client objects to any such changes, Crowe will work with Client in good faith to find a mutually agreeable resolution.

7. Transfers.

a. **EU Transfers.** Client (as "**data exporter**") and Crowe (as "**data importer**"), with effect from the commencement of the relevant transfer, when necessary, shall enter into the SCCs in respect of any transfer (or onward transfer) from Client to Crowe (or onward transfer) where such transfer is not allowed under the DPF or would otherwise be prohibited by applicable Data Privacy Laws (or by the terms of data transfer agreements put in place to address Data Privacy Laws).

b. **UK Transfers.** Client (as "**data exporter**") and Crowe (as "**data importer**"), with effect from the commencement of the relevant transfer, when necessary, shall enter into the UK IDTA in respect of any transfer (or onward transfer) from Client to Crowe (or onward transfer) where such transfer is not allowed under the DPF or would otherwise be prohibited by UK Data Privacy Laws (or by the terms of data transfer agreements put in place to address UK Data Privacy Laws).

8. Assistance. Crowe will reasonably cooperate with Client in responding to or addressing any verified request from a consumer or data subject, a data privacy authority with jurisdiction, or the Client, as necessary to enable Client to comply with its obligations under applicable data protection laws and to the extent related to Personal Data processed by Crowe. Client will promptly reimburse Crowe for any out-of-pocket expenses and professional time (at Crowe's then-current hourly rates) incurred in connection with providing such cooperation. Client will provide prompt written notice to Crowe, including reasonable detail and instructions, regarding any action required of Crowe under this Section. Crowe will not be obligated to take any such action without sufficient written direction and coordination from Client, and only to the extent such assistance is reasonable in light of the nature of the request, the processing activities, and Crowe's role under applicable Data Privacy Laws.

9. Audit. Once per year during the term of the Agreement, Client may audit Crowe's compliance with this Addendum provided that such audits solely consist of Crowe's obligation to respond to reasonable written cybersecurity and data protection audit questionnaires with at least thirty (30) days' advance notice.

10. Miscellaneous.

a. In the event of any conflict between the data privacy provisions of this Addendum and the provisions of the Agreement, the data privacy provisions of this Addendum shall prevail. In the event of any conflict between the data privacy provisions of this Addendum and the SCCs, the SCCs shall control and take precedence. If there is any conflict between the data privacy provisions of this Addendum and a

Business Associate Agreement entered into between the parties ("**BAA**"), to the extent the Client has transferred Protected Health information to Crowe, then the BAA shall control and take precedence.

b. Notwithstanding anything to the contrary in the Agreement or this Addendum and to the maximum extent permitted by law, each party's and all of its affiliates' liability, taken together in the aggregate, arising out of or related to this Addendum, the SCCs or any other data protection agreements in connection with the Agreement (if any), whether in contract, tort or under any other theory of liability, shall remain subject to the limitation of liability section of the main body of the Agreement and any reference in such section to the liability of a party means the aggregate liability of that party and all of its affiliates under the Agreement and this Addendum, including all exhibits and schedules hereto. Client agrees that any regulatory penalties incurred by Crowe that arise in connection with Client's failure to comply with its obligations under this Addendum or any laws or regulations including Data Privacy Laws shall reduce Crowe's liability under the Agreement as if such penalties were liabilities to Client under the Agreement.

c. If Client must transfer Client Personal Data to Crowe and this Addendum does not adequately address the transfer, the Parties shall, in good faith and as required by Data Privacy Laws, amend or update this Addendum's terms accordingly.

d. This Addendum is effective and legally binding without the need for a physical or electronic signature by either Party, upon its incorporation into the Agreement by reference, including by hyperlink or other written acknowledgment. By continuing to receive or use the Services, Client agrees to the terms of this Addendum.

Schedule 1: Description of Processing of Client Personal Data

Data exporter: The entity identified as "Client" in the Agreement.

Contact person's name, position and contact details: The signer of the Agreement on behalf of the Client, their position, address, and contact details set forth therein.

Activities are set forth in Section B. below.

Please see the Agreement for the signature and date.

Role (controller/processor): Controller

Data importer: Crowe LLP

Contact person's name, position and contact details: The signer of the Agreement on behalf of the Crowe, their position, address, and contact details set forth therein.

Activities are set forth in Section B. below.

Please see the Agreement for the signature and date.

Role (controller/processor): Controller/Processor (depending on the nature of the relationship)

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

_____

If Client has not completed the above section, Client shall be deemed to have declared that the categories of data subjects are including but not limited to consumer customers, prospective consumer customers, professionals, commercial customers, employees, contractors, suppliers.

Categories of personal data transferred

_____

If Client has not completed the above section, Client shall be deemed to have declared that the categories of personal data transferred include but not limited to individual contact information, unique identifiers, information pertaining to consumer transactions, information pertaining to commercial transactions, human resources data, online or technical information.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Subject to the terms of this Addendum, and solely to the extent necessary to perform the Services, Client may include 'special categories of personal data' or sensitive personal data (as described by applicable Data Privacy Law) as set forth in the Agreement. This data may include but is not limited to race, ethnicity, political opinions, religious beliefs, and health data.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous or as-needed depending on the nature of the Services.

Nature of the processing

As set forth in the Services to the Agreement.

Purpose(s) of the data transfer and further processing

To perform the Services set forth in the Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

During the term as set forth in the Agreement.

For transfers to (sub) processors, also specify subject matter, nature and duration of the processing

To perform the Services set forth in the Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The Data Protection Commission of Ireland shall act as a competent supervisory authority.

Schedule 2: Crowe Security Measures

Crowe's Information Security Statement is located at https://www.crowe.com/iss.

Schedule 3: Sub-Processors

Crowe's Sub-Processor List is located at https://www.crowe.com/sub-processor-list.

EXHIBIT A

STANDARD CONTRACTUAL CLAUSES

As necessary and set forth in Section 5.1 of the Addendum, the parties will enter in the SCCs with the following configuration of modules, options, and optional clauses:

1. The SCCs will be modified consistent with Module 1 (Controller to Controller), where Crowe is a controller for the data and Module 2 (Controller to Processor), where Crowe is a processor for the data, removing other modules from the SCCs.
2. The optional docking clause, Clause 7, will be included.
3. For Module 2: option 2 of Clause 9(a) will be selected, and the time specified will be 30 days.
4. The optional language under Clause 11(a) will be deleted.
5. Option 1 will be selected under Clause 17 and the Member State will be: Ireland.
6. The Member State for Clause 18(b) will be: Ireland.
7. The information required by Annex I will be completed using Schedule 1 to the Addendum.
8. The information required by Annex II will be completed using Schedule 2 to the Addendum.
9. The information required by Annex III will be completed using Schedule 3 to the Addendum.

EXHIBIT B

UK ITDA

As necessary and set forth in Section 5(b) of the Addendum, the parties will enter in the UK ITDA and complete the required tables as follows:

Part 1: Tables

Table 1: Parties

Start date	The Effective Date of the Addendum	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	See Schedule 1 to the Addendum	See Schedule 1 to the Addendum
Key Contact	See Schedule 1 to the Addendum	See Schedule 1 to the Addendum
Signature (if required for the purposes of Section 2)	See Addendum Signature Page	See Addendum Signature Page

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☐ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Addendum Effective Date Reference (if any): Other identifier (if any): Addendum, Exhibit B Or ☒ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:					
Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data

						collected by the Exporter?
1						
2	X	X		General	30 days	
3						
4						

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: *Set forth in Schedule 1 to the Addendum*
Annex 1B: Description of Transfer: *Set forth in Schedule 1 to the Addendum*
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: *Set forth in Schedule 2 to the Addendum*
Annex III: List of Sub-processors (Modules 2 and 3 only): *Set forth in Schedule 3 to the Addendum*

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☒ Importer ☒ Exporter ☐ neither Party