DATA PROCESSING ADDENDUM

(the "***DPA***")

to DMI General Service Agreement (the "***Addendum***") between **The Client (**the **"Controller")**and **Digital Marketing Institute** (seat: Duncairn House, 14 Carysford Avenue, Blackrock, Co. Dublin, Ireland) as data processor (the "***Processor***" or *"**Provider**"*)

1. APPLICABLE DATA PROTECTION RULES

a. The processing of personal data under this Addendum is subject to the EU Regulation No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of natural persons with regard to the processing of personal data and on the free movement of such data (the General Data Protection Regulation or "***GDPR****"*) and any national implementing or complementing rules and regulations in the territory where services will be provided (the "***Data Protection Rules***").

b. The terms "***personal data***", "***data subject***", "***controller***", "***processor***", "***processing***" and "***third party***" shall have the meaning given to these terms under the applicable Data Protection Rules.

c. For the performance of the Services under the Addendum, the Processor may process personal data (the "***Personal Data***") on behalf of Controller. The processing activities of the Processor are as described in Annex 1 to this DPA.

2. OBLIGATIONS OF THE PROCESSOR

a. The Processor acknowledges that the Personal Data transferred to it are subject to the Data Protection Rules. The Processor shall only process the Personal Data (i) as part of and to the extent necessary for the performance of the Addendum, (ii) in accordance with this Addendum and the Data Protection Rules, and (iii) in accordance with and only on documented instructions from Controller. The Processor shall not use the Personal Data for any of its own secondary purposes.

b. The Processor must inform its employees and staff of the relevant obligations under this Addendum and Controller's instructions. The Processor shall ensure and monitor its employees' compliance with such obligations and instructions.

c. The Processor must implement appropriate technical, physical and organizational security measures to protect the Personal Data under its control against accidental or unlawful destruction or accidental loss, alteration, unauthorized or unlawful storage, processing, access or disclosure, and any other unauthorized processing of the Personal Data. These security measures should meet the best industry standards and must be updated from time to time to provide an adequate level of protection taking into account the risks involved in the processing and the nature of the Personal Data to be secured. The Processor's implemented security measures (technical and organizational measures) can be found in Annex 2. The Processor shall have in place a security plan (see the security plan in Annex 3) and conduct regular tests, assessments and evaluations of the effectiveness of such measures and report to Controller.

d. The Processor shall maintain a written (or electronic) record of all categories of processing activities carried out on behalf of Controller. Such a register shall include, at least, all information referred to in Article 30.2 of the GDPR.

e. The Processor shall take all technical and organisational measures required to comply with the Data Protection Rules, including the implementation of security measures, carrying out privacy impact assessments as well as allowing the data subjects to exercise their rights under the Data Protection Rules. In addition, the Processor shall assist Controller in complying with its obligations under applicable Data Protection Rules or requests it receives from supervisory authorities.

f. The Processor shall promptly inform Controller:

i. of any complaint, request or enquiry from a data subject regarding the processing of its Personal Data and/or its rights under the Data Protection Rules and, in such a case, assist Controller with the fulfilment of its obligation to address/respond to such complaints, requests or enquiries;

ii. of any inquiry it receives from public authorities for an inspection or audit of the processing of Personal Data.

g. The Processor shall immediately take all appropriate measures to remedy any breach of security or data breach and provide Controller with all information at its disposal relevant to the data security breach, including, without limitation, the nature and scope of the Personal Data affected by said breach, the individuals concerned, the technological protection measures that had been put in place beforehand (e.g., whether the data was pseudonymized and/or encrypted), the measures taken or recommended to mitigate the possible adverse effects of the security breach, and any other information that might be or become relevant in order for Controller to comply with statutory or other security breach notification duties. The Processor shall prepare a data breach report and provide the Controller with that report within reasonable period of time from the occurrence of the breach. The Processor shall also fully cooperate with Controller in the framework of any consequential action (e.g. notification of the breach to the supervisory authority and to the data

subject) taken by the latter in relation to that breach.

3. CONFIDENTIALITY

a. The Processor shall keep confidential and not disclose any Personal Data to third parties without the consent of Controller. Nevertheless, the Processor may communicate the Personal Data to third parties where such disclosure is required by applicable law. The Processor shall provide Controller with prior notice where it is required to disclose the Personal Data to a third party pursuant to applicable law.

b. The Processor shall only disclose the Personal Data or allow access to the Personal Data to those of its employees or staff who require such disclosure/access to enable the Processor to perform its obligations under the Addendum, provided that these persons have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. The Processor shall keep a record of any disclosure made in accordance with this clause 12 and shall procure that any such persons are subject to written contractual obligations concerning the Personal Data which are no less onerous than those imposed on the Processor under this DPA.

c. The Processor shall not copy the Personal Data except insofar as this is necessary for the performance of the Addendum.

4. SUB-PROCESSING

a. As of the Addendum Effective Date, the Controller hereby authorises that the Processor to engage Sub-Processors for the fulfilment of its processing obligations; provided, that the Processor shall require any Sub-Processor to comply with Data Protection Laws and with the obligations arising from this Addendum.

b. The Processor will remain fully liable to Controller for any sub-processor that fails to fulfil its obligations under this DPA or the applicable Data Protection Rules.

5. INTERNATIONAL TRANSFER OF PERSONAL DATA

a. The Processor shall not transfer Personal Data under its control to, or otherwise make Personal Data under its control accessible in, countries outside the European Economic Area not recognised as providing an adequate level of protection under the Data Protection Rules, without the prior approval of Controller.

6. INFORMATION AND AUDITS

a. The Processor shall, at the request of Controller, provide all information necessary to demonstrate its compliance with the Data Protection Rules and with its obligations as stated under this DPA.

b. In addition, upon reasonable notice by Controller, the Processor shall free of charge allow for and contribute to audits, including inspections, conducted during normal business hours by or on behalf of Controller. If such an audit demonstrates that the Processor has breached any of its obligations under this DPA, it shall immediately rectify that breach.

7. DELETION OR RETURN OF PERSONAL DATA

a. The Processor shall delete or return, at the choice of Controller, all Personal Data at the Controller's first request and, in any case, at the end of the provision of services relating to the processing. The Processor shall not keep Personal Data longer than is necessary for the purpose of performing its obligations under the Addendum, unless required by law, and implement technical measures to comply with this obligation.

8. MISCELLANEOUS

a. If any provision of this DPA is held to be illegal, invalid or unenforceable under any present or future law, this will not affect the validity of the remaining provisions of this DPA. The Parties will cooperate to review or amend this DPA as required to reflect the initial intention in accordance with the applicable rules.

b. All clauses of this DPA should be interpreted in accordance with the Data Protection Rules that are or may become applicable during the term of this DPA.

c. The Addendum shall be governed by Irish law. Disputes relating to this Addendum will be exclusively submitted to the competent Irish courts.

d. This DPA shall apply as from the date of signing and continue to apply as long as the Processor processes personal data on behalf of Controller.

ANNEX 1:
SCOPE OF THE SERVICES AND OF THE DATA PROCESSING

1. THE SERVICES

The Services include the following (please specify):

The purpose of the Services is the subscription and access to the e-Learning databases of the Provider/Processor for the authorized users of the Client/Controller. The Provider has agreed to provide the Client/Controller with online access to the following e-Learning databases for the authorized users of the Client/Controller:

- Education and Training Courses
- Professional Resources
- Continuous Professional Development Programs

2. DATA SUBJECTS

The Personal Data concern the following categories of data subjects (please specify):

- Authorized users of the Controller with online access to the e-Learning training.
- Employees, advisors or other representatives of Controller, whose personal data are processed during and after the existence and in connection with the performance of the Addendum and this DPA.

3. CATEGORIES OF PERSONAL DATA

a. The Personal Data concerns the following categories of data (please specify):

- **Identification Data:** PII, Electronic Identification Data
- **Personal Characteristics:** Personal details
- **Private Habits:** Platform and media use
- **Education and training:** Academic curriculum, professional qualifications and experience
- **Professional and employment**: Current employer, training for the position, use of technology
- **Video recordings:** Images

b. The Personal Data concern the following special categories of data (please specify):

- **Not applicable**

4. PURPOSE OF THE DATA PROCESSING

The Personal Data will be processed for the following purposes (please specify):

- **General purposes:** User management
- **Education:** Student administration
- **Market Research and Statistical Research, consistent with the original collection purpose**
- **Trade:** Direct Marketing and User Engagement

ANNEX 2
LIST OF PROCESSOR'S SECURITY MEASURES

The Digital Marketing Institute has put in place a number of security measures to safeguard the data that we are entrusted with, to minimise any risks that may impact our operations and data, and to ensure a universal level of understanding around policies and best practices surrounding the management and usage of data.

A number of policies have been developed over the last number of years to govern our IT Service Management, created in line with ITIL and ISO 27001 frameworks and practices. These policies are put in place to protect the company's infrastructure and data processing activities, and members of staff are briefed and trained around what to do and what not to do when conducting their day to day business operations.

Aside from IT governance policies which are followed by all personnel within the company, we have put in place a number of safeguards in place, which include but are not limited to the following;

1. Encryption as standard all company hardware
2. Secure password policies for all staff accounts
3. Automated backups as part of our data recovery and business continuity plans
4. Firewalls and Network security and monitoring tools
5. Mobile and Teleworking policies and tools
6. Acceptable use
7. Responsibility for assets
8. Prohibited Activities
9. Taking assets off-site
10. Return of assets upon termination of contract
11. Backup procedure
12. Antivirus protection
13. Authorizations for information system use
14. User account responsibilities
15. Password responsibilities
16. Internet use
17. E-mail and other message exchange methods
18. Copyright
19. CCTV
20. Visitor Log Book
21. Clear Desk Policy
22. Lockable Storage Lockers

ANNEX 3

PROCESSOR'S SECURITY PLAN

The purpose of this section is to outline a number of the organisational measures and policies that are in place to ensure secure and continued operation of all Digital Marketing Institute IT infrastructure components and communication technology.

This section outlines a number of our processes in relation to certain aspects of our operations.

1. **CHANGE MANAGEMENT**

Each change to operational or production systems must be done so in accordance with the following protocol:

a. change may be proposed by a Digital Marketing Institute Head of Department using the change request form

b. change must be authorized by Digital Marketing Institute CTO, who must assess its justification for business and potential negative security impacts

c. changes must be implemented by Digital Marketing Institute IT Department.

d. Digital Marketing Institute Head of Department is responsible for checking that the change has been implemented in accordance with the outlined requirements.

e. Digital Marketing Institute IT Department is responsible for testing and verifying the system's stability – the system must not be put into production before thorough testing has been conducted

f. implementation of changes must be reported to the following Digital Marketing Institute persons: CTO, CFO, IT Manager, Head of Department.

Change records are kept within a Change Management System.

2. **Backup Procedure**

a. Backup copies must be created for all critical and required operational system with the back up frequency specified within our detailed backup documentation

b. The IT Manager is responsible for the execution of backup procedures and the creation of information backups, and software and system images.

c. Logs of the backup process are automatically created on systems where the backup copy is made.

3. **Testing Backup Copies**

a. Backup copies and the process of their restoration must be tested at least once every six months by executing the data restoration process on the backup server or on a system test instance where applicable, and checking that all data has been successfully recovered.

b. The IT Manager is responsible for testing backup copies. Records on testing backup copies are kept in a electronic format on the internal shared drive.

4. **Network security management**

The IT Manager is responsible for managing and controlling the computer networks, for ensuring the security of information in networks, and for protecting the services connected to the networks from unauthorized access. It company policy that the network is managed in such a way that the IT Manager is required

a. to separate the operational responsibility for networks from the responsibility for sensitive applications and other systems
b. to protect sensitive data passing over the public network by protect the data with encryption.
c. to protect sensitive data passing over wireless networks by using of WPA2 protocol
d. to protect equipment connecting to the network from remote locations by user of VPNs
e. to segregate traffic coming in from mobile devices, set up unique firewall policies, static routes, Virtual Local Area Networks, etc.
f. to ensure the availability of network services by providing adequate bandwidth and needed bypasses in case of network failure, monitoring all points within the network.

5. **Network services**
   a. The IT Manager has defined security features and the level of expected services for all network services, whether these services are provided in-house or outsourced – such requirements should be documented with service providers.
   b. If the network services are outsourced, then the requirements must be specified in the Addendum with the service provider.
6. **System monitoring**
   a. Based on risk assessment findings, Digital Marketing Institute CTO decides which logs will be kept on which systems and for which systems, and how long they will be stored. Logs must be kept for all administrators and system operators on sensitive systems.
   b. The IT Manager is responsible for monitoring the logs of automatically reported faults on a daily basis, as well as to register faults reported by users, to analyse why errors occurred and to take appropriate corrective actions.
   c. The IT Manager is responsible for regularly reviewing logs in order to monitor the activities of users, administrators and system operators. The review is conducted at intervals prescribed by Digital Marketing Institute CTO, who determines and selects the records to be reviewed, and how the implemented review will be recorded. Digital Marketing Institute CTO must be informed about the results of the review.