This document is part of the Data Processing Agreement.

ANNEX 1 PART III

THIS PART III OF ANNEX 1 SHALL APPLY WHERE THE SERVICES DESCRIPTION PAGE INDICATES THAT TCM IS COMPANY'S PROCESSOR OR SUBPROCESSOR (THE "TCM PROCESSOR SERVICES")

1. Relationship of the Parties

1.1 In relation to all Company Data, TCM acknowledges that, as between the Parties, Company is either (a) the Controller of Company Data, and that TCM, in providing or using the Services is acting as a Processor on behalf of the Controller; (b) or Company is a Processor of Company Data, and that TCM, in providing or using the Services is acting as a Subprocessor on behalf of Company.

" Company Data " means any and all Personal Data (as that term is defined in EU Data Protection Law) that is processed by TCM or its sub processors on behalf of Company in the performance of the TCM Processor Services and its other obligations under the MSA.

1.2 The subject-matter and duration of the Processing carried out by the Processor on behalf of the Controller, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects are described in Exhibit 1 to this Annex 1 Part III .

1.3 Company represents and warrants that: (a) its Processing instructions comply with all Applicable Data Protection Laws; and (b) it has obtained and maintains all legally required notices, consents and permissions for the Processing and transfer of all Personal Data provided to TCM. Company acknowledges that, taking into account the nature of the Processing, TCM is not in a position to determine whether Company's instructions infringe Applicable Data Protection Laws .

2. Protection of Personal Data

2.1 In respect of the Processing of Personal Data by TCM in connection with the TCM Processor Services where EU Data Protection Law applies, TCM is responsible for and shall comply with Applicable Data Protection Law and agrees that it shall:

(a) process the Company Data only on written instructions from Company (which may, in particular, be given electronically or through the functionality of the Services), including with regard to transfers of Personal Data to a third country or an international organisation, unless required to do so by European Union or Member State law to which TCM is subject; in such a case, TCM shall inform Company of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest;

(b) implement and maintain the technical and organisational measures set out in Exhibit 3 and take all measures required pursuant to Article 32 of the GDPR including all organisational and technical security measures necessary to protect against unauthorised or accidental access, loss, alteration, disclosure or destruction of Company Data, in particular where the Processing involves the transmission of data over a network, and against all other unlawful forms of Processing;

(c) treat all Company Data processed by it on behalf of Company as confidential and ensure that persons authorised to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, even after the end of their employment contract or at the end of their assignment or engagement;

(d) cooperate as reasonably requested by Company and implement appropriate technical and organisational measures to enable Company to comply with any exercise of rights by a Data Subject under Applicable Data Protection Law in respect of Personal Data processed by TCM under the MSA (including, without limitation, in relation to the retrieval and/or deletion of a Data Subject's Personal Data);

(e) without prejudice to Section 3 of the Terms and Conditions (International Transfers) of this Agreement, not access or transfer outside the European Economic Area (" EEA ") any Personal Data without the prior written consent of Company unless in accordance with EU Data Protection Law;

(f) provide (at no additional cost to Company) Company with all resources and assistance as are reasonably required by Company in connection with the Services performed by TCM under the MSA for Company to discharge its duties pursuant to Articles 32 to 36 of the GDPR including, but not limited to, promptly at the request of Company provide information in respect of any data protection impact assessment which Company conducts and assist Company with any prior consultations with any supervisory authority;

(g) at the choice of Company, delete or return all the Company Data to Company after the end of the provision of the TCM Processor Services, and delete existing copies unless European Union or Member State law requires storage of the Company Data;

(h) make available to Company at its request all information necessary to demonstrate compliance with the obligations laid down in this Agreement and Article 28 of the GDPR including without limitation a detailed written description of the technical and organisational methods employed by TCM and its Subprocessors (if any) for the Processing of Personal Data; and

(i) immediately inform the Controller if, in the Processor's opinion, an instruction from the Controller infringes Applicable Data Protection Law.

2.2 Company may exercise its audit right under the Applicable Data Protection Laws in relation to Company Data through a request that TCM initially provide Company with a summary copy of TCM audit report(s) related to TCM's technical and organizational security measures. For the avoidance of doubt, such reports shall be subject to the confidentiality provisions of the MSA. If following TCM's delivery of such reports, Company wishes further information necessary for TCM to demonstrate its compliance with its security obligations herein, then TCM agrees at the request of Company to submit its data processing facilities (including all equipment, documents and electronic data relating to the Processing of Company Data) and/or any location from which Company Data can be accessed by Processor for audit to ascertain and/or monitor compliance with this Agreement and Applicable Data Protection Law. Such audit shall be

carried out, with reasonable notice and during regular business hours and under a duty of confidentiality, by Company and/or by a third party appointed by Company.

3. Notification of Security Incident

3.1 TCM will notify Company without undue delay (and, in any event within forty-eight (48) hours) upon becoming aware that an actual Security Incident involving the Company Personal Data in TCM's possession or control has occurred, as TCM determines in its sole discretion. TCM's notification of or response to a Security Incident under this Section 3 (Notification of Security Incident) shall not be construed as an acknowledgment by TCM of any fault or liability with respect to the Security Incident.

3.2 TCM will, as soon as reasonably possible, provide Company with at least the following information with respect to the Security Incident affecting Company Data: (i) a description of the cause and nature of the Security Incident including the categories and approximate numbers of Data Subjects (including the number of Company Data Subjects) concerned and the categories and approximate number of Personal Data records concerned; (ii) the measures being taken to contain, investigate and remediate the Security Incident; (iii) the likely consequences and risks for Company and its Data Subjects as a result of the Security Incident; (iv) any mitigating actions taken; and (v) a proposed plan to mitigate any risks for Data Subjects and/or Company as a result of the Security Incident.

3.3 TCM will, in connection with any Security Incident affecting Company Data: (i) quickly and without delay, take such steps as are necessary to contain, remediate, minimise any effects of and investigate any Security Incident (and without destroying any evidence) and to identify its cause (ii) co-operate with Company and provide Company with such assistance and information as it may reasonably require in connection with the containment, investigation, remediation and/or mitigation of the Security Incident; and (iii) immediately notify Company in writing of any request, inspection, audit or investigation by a supervisory authority or other authority.

3.4 TCM agrees that it will not communicate with any third party, including but not limited to the media, vendors, consumers and affected individuals regarding any Security Incident involving Company Data without the express written consent and direction of Company.

4. Subprocessing

4.1 TCM may, subject to compliance with Section 4.2, continue to use those Subprocessors already engaged by TCM and as identified to Company prior to commencement of the Agreement to process any Company Data. TCM may, subject to compliance with Section 4.2, engage an additional or replace an existing Subprocessor to process Personal Data provided that it notifies Company of any intended use or replacement of a Subprocessor by email to contact@thinkclevermedia.com.com (" email notification ") thirty (30) days in advance of, as applicable, the engagement or replacement of the Subprocessor concerned, unless Company objects in writing to the proposed use or replacement of the relevant Subprocessor within thirty (30) days of receipt of the email notification (in which case TCM shall not, as applicable, use or replace the Subprocessor concerned).

4.2 TCM shall, where it engages any Subprocessor in accordance with Section 4.1; (i) only use a Subprocessor that has provided sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR and the Agreement and ensure the protection of the rights of Data Subjects; and (ii) impose, through a legally binding contract between TCM and Subprocessor, data protection obligations no less onerous than those set out in the Agreement (including those that apply pursuant to the Controller to Processor Standard Clauses) on the Subprocessor, in particular providing sufficient guarantees to implement appropriate technical and organisational

measures in such a manner that the processing will meet the requirements of the GDPR. TCM acknowledges and agrees that if any Subprocessor fails to fulfil its obligations in the contract between TCM and Subprocessor, TCM shall remain fully liable to Company for the performance of the Subprocessor's obligations.

5. Liability and Payment of Compensation

Without prejudice to the provisions of the MSA, TCM shall defend, indemnify and hold Company harmless and keep Company indemnified, on demand from and against any and all damages (including non-material damage) incurred by Company as a result of TCM's and/or its employees or representatives unauthorised and/or unlawful Processing, or accidental loss, disclosure, destruction or damage to any Company Data obtained from (or held by TCM or its personnel on behalf of) Company, save where such loss, disclosure, destruction or damage was carried out or incurred at the Company's request. TCM shall be liable for and shall indemnify Company and its employees and agents from and against all damages (including non-material damage) which Company may suffer consequent upon breach of Applicable Data Protection Law, recklessness or wilful default of TCM, its employees or agents. In no event shall TCM's total liability to Company under this Annex 1 Part III exceed €5,000,000.00.

EXHIBIT 1 DETAILS OF PROCESSING ACTIVITIES

Subject Matter	Processing carried out in connection with the provision of the Services (as defined in the MSA).	
Duration	The Term plus the period from the expiration of the Term until deletion of Company Data by TCM in accordance with the terms of this Agreement.	
Nature & Purpose of the Processing	TCM will process, including as applicable to the Processor Services and the instructions set forth in Section II of this Annex 1 Part III, Company Data for the purpose of providing the Processor Services and any related technical support to Company in accordance with this Agreement.	
Categories of Data Subjects	Data Subjects about whom TCM collects Personal Data in its provision of the Processor Services; and Data Subjects about whom Personal Data is transferred to TCM in connection with the Processor Services by, at the direction of, or on behalf of Company.	☐
	Other	☐
	If Other, Please Specify:	
Types of Personal Data	The Company Data may include, but shall not be limited to, the following types of Personal Data depending on the Processor Services: IP addresses and similar unique IDs such as cookie IDs and device IDs	☐
	Other	☐
	If Other, Please Specify:	

EXHIBIT 2

APPENDIX 1 TO THE CONTROLLER TO PROCESSOR STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter
The data exporter is (please specify briefly your activities relevant to the transfer): TCM as defined in this Agreement.

Data importer
The data importer is (please specify briefly activities relevant to the transfer):
The legal entity of Company that has executed the Standard Contractual Clauses as a Data Exporter and all Affiliates established in the EEA.

Data subjects
The personal data transferred concern the following categories of data subjects (please specify):
Data Subjects about whom Company collects Personal Data in its provision of the Processor Services; and Data Subjects about whom Personal Data is transferred to Company in connection with the Processor Services by, at the direction of, or on behalf of TCM.

Categories of data
The personal data transferred concern the following categories of data (please specify):
The TCM Data provided by TCM to Company in connection with its use of the Services. The TCM Data may include, but shall not be limited to, the following types of Personal Data depending on the Processor Services: IP addresses and similar unique IDs such as cookie IDs and device IDs.

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data (please specify):
N/A

Processing operations
The personal data transferred will be subject to the following basic processing activities (please specify):
The objective of Processing of Personal Data by Company is the performance of the Services under the MSA.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached): As per Exhibit 3.

EXHIBIT 3
TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

TCM will implement and maintain the following technical and organisational security measures, in particular:

TCM Information Security Overview

TCM takes information security seriously. This information security overview applies to TCM's corporate controls for safeguarding personal data, which is processed in connection with delivery of our services. TCM's information security program enables the workforce to understand their responsibilities. Some customer solutions may have alternate safeguards outlined in the statement of work as agreed with each customer.

Security Practices

TCM has established comprehensive information regarding industry standard security governance framework.

Organizational Security

It is the responsibility of the individuals across the organization to comply with these practices and standards. To facilitate the corporate adherence to the practices and standards, the function of information security provides:

- Strategy and compliance with policies/standards and regulations, awareness and education, risk assessments and management, contract security requirements management, application and infrastructure consulting, assurance testing and drives the security direction of the company.

- Security testing, design and implementation of security solutions to enable security controls adoption across the environment.

- Security operations of implemented security solutions, the environment and assets, and manage incident response.

Asset Classification and Control

TCM's practice is to track and manage physical and logical assets. Examples of the assets that TCM IT might track include:

- Information Assets, such as identified databases, network resiliency and redundancy architecture, data classification, archived information.

- Software Assets, such as identified applications and system software.

- Physical Assets, such as identified servers, desktops/laptops, backup/archival tapes, printers and communications equipment. The assets are classified based on business criticality to determine confidentiality requirements. Technical, organizational and physical safeguards may include controls such as access management, encryption and monitoring.

Personnel Security and Training

As part of the employment process, employees undergo a screening process applicable per regional law. Employees are bound to follow TCM's policies and procedures and breaking or not following these will result in disciplinary actions up to and including termination based on local law. Additionally TCM service providers are contractually bound to adhere to the same policies and procedures as full time employees.

Operations Management

The IT organization manages changes to the corporate infrastructure, systems and applications through a centralized change management program, which may include, testing, business impact analysis and management approval where appropriate.

To protect against malicious use of assets and malicious software, additional controls may be implemented based on risk. Common controls may include, but are not limited to, additional information security policies and standards, restricted access, designated development and test environments, virus detection on endpoints, email attachment scanning, system compliance scans, information handling options for the data exporter based on data type, network security, and system and application vulnerability scanning.

Incident Response

TCM continually monitors and reports on potential security related events whether that be directly or using a 3rd Party to prompt TCM. TCM utilizes multiple protection methods across the enterprise to identify, track, block, and remediate vulnerabilities and potential breaches. Additionally, there is an established process for incident response and a web page with instructions for easy reference.

Access Controls

Access to corporate systems is restricted, based on procedures to ensure appropriate approvals. This also applies to remote access and wireless computing access to systems being equally restricted.

System Development and Maintenance

Publicly released third party vulnerabilities are reviewed for applicability in the TCM environment. Based on risk to TCM's business and customers, there are predetermined time frames for remediation. Code reviews are used in the development environment prior to production.

Compliance

The company works to identify regional laws, regulations applicable to TCM compliance. Actions may include but are not limited to; Internal and external legal counsel consultation, internal controls assessment, contract management, security awareness, security consulting, combine to drive compliance with these requirements.