



This document is part of the Data Processing Agreement.

ANNEX 1 PART II

THIS PART II OF ANNEX 1 SHALL APPLY WHERE THE SERVICES DESCRIPTION PAGE INDICATES THAT

(A) TCM IS A CONTROLLER AND COMPANY IS A PROCESSOR, OR
(B) TCM IS A PROCESSOR AND COMPANY IS A SUBPROCESSOR,
((A)& (B) TOGETHER THE “ PROCESSOR SERVICES ”)

1. Relationship of the Parties

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

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

1.2 The subject-matter and duration of the Processing carried out by the Processor in connection with the Processor Services, 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 II .

2. Protection of Personal Data

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

(a) process the TCM Data only on written instructions from TCM (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 Company is subject; in such a case, Company shall inform TCM 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 other measures required pursuant to Article 32 of the GDPR including all organizational

and technical security measures necessary to protect against unauthorised or accidental access, loss, alteration, disclosure or destruction of TCM 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 TCM Data processed by it on behalf of TCM 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 requested by TCM and implement appropriate technical and organisational measures to enable TCM to comply with any exercise of rights by a Data Subject under Applicable Data Protection Law in respect of Personal Data processed by Company 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 TCM;

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

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

(h) make available to TCM 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 Company 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 agrees at the request of TCM to submit its data processing facilities (including all equipment, documents and electronic data relating to the Processing of TCM Data) and/or any location from which TCM Data can be accessed by Processor for audit to ascertain and/or monitor compliance with this Agreement and Applicable Data Protection Law which audit shall be carried out, with reasonable notice and during regular business hours and under a duty of confidentiality, by TCM and/or by a third party designated by TCM.

3. Notification of Security Incident

3.1 Company will notify TCM without undue delay (and, in any event within forty-eight (48) hours) upon becoming aware that an actual Security Incident has occurred, as Company determines in its sole discretion. Company'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 Company of any fault or liability with respect to the Security Incident.

3.2 Company will, as soon as possible, provide TCM with at least the following information

with respect to the Security Incident affecting TCM 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 TCM 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 TCM 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 TCM as a result of the Security Incident.

3.3 Company will, in connection with any Security Incident affecting TCM 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 TCM and provide TCM 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 TCM in writing of any request, inspection, audit or investigation by a supervisory authority or other authority.

3.4 Company 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 connected to the Processor Services without the express written consent and direction of TCM.

4. Subprocessing

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

4.2 Company 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 Company and Subprocessor, the same data protection obligations as set out in the Agreement (including without limitation, those that apply pursuant to the Controller to Processor Standard Clauses), 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. Company acknowledges and agrees that if any Subprocessor fails to fulfil its obligations in the contract between Company and Subprocessor, Company shall remain fully liable to TCM for the performance of the Subprocessor’s obligations.

5. Liability and Payment of Compensation

Notwithstanding the provisions of the MSA, Company shall defend, indemnify and hold TCM harmless and keep TCM indemnified, on demand from and against any and all actual or alleged claims and damages incurred by TCM as a result of Company’s and/or its employees or representatives (including without limitation any Subprocessors) unauthorised and/or unlawful Processing, or accidental loss, disclosure, destruction or damage to any TCM Data obtained

from (or held by Company or its personnel on behalf of) TCM, save where such loss, disclosure, destruction or damage was carried out or incurred at TCM's request. Company shall be liable for and shall indemnify TCM and its employees and agents from and against all damages (including non-material damage) which TCM may suffer consequent upon any breach of Applicable Data Protection Law, recklessness or wilful default of Company, its employees or agents.

6. Insurance

Company shall take out and maintain insurance policies to the value sufficient to meet its liability and that of its Subprocessors under or in connection with this Agreement, and in no event shall such amount be less than €5,000,000.00. Within thirty (30) days of execution of this Agreement, Company shall provide proof of such insurance in the form of a certificate of insurance for data breach liability and which names TCM as an additional insured.

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 TCM Personal Data by Company in accordance with the terms of this Agreement.	
Nature & Purpose of the Processing	Company will process, including as applicable to the Processor Services and the instructions set forth in Section II of this Annex 1 Part II, TCM Data for the purpose of providing the Processors Services and any related technical support to TCM in accordance with this Agreement.	
Categories of Data Subjects	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.	<input type="checkbox"/>
	Other	<input type="checkbox"/>
	If Other, Please Specify:	
Types of Personal Data	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	<input type="checkbox"/>
	Other	<input type="checkbox"/>
	If Other, Please Specify:	

EXHIBIT 2

APPENDIX 1 TO THE CONTROLLER TO PROCESSOR STANDARD CONTRACTUAL CLAUSES

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):

<https://www.contentignite.com/gdpr/data-safety/>

EXHIBIT 3: TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

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

<https://www.contentignite.com/gdpr/data-safety/>