DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**DPA**") forms part of the Master Service Agreement ("**Agreement**") entered by and between you, the Customer (as defined in the Agreement) (collectively, "**you**", "**your**", "**Customer**"), and Content Square SAS. ("**Contentsquare**", "**us**", "**we**", "**our**") to reflect the parties' agreement with regard to the Processing of Personal Data by Contentsquare solely on behalf of the Customer. Both parties shall be referred to as the "**Parties**" and each, a "**Party**".

Capitalized terms not defined herein shall have the meanings assigned to such terms in the Agreement.

Unless otherwise explicitly stated herein, the terms of the Agreement shall be incorporated as part of this DPA and any claims brought under this DPA shall be subject to the terms of the Agreement. In the event of any conflict between certain provisions of this DPA and the provisions of the Agreement, the provisions of this DPA shall prevail over the conflicting provisions of the Agreement solely with respect to the Processing of Personal Data.

1. DEFINITIONS

1.1 Definitions:

(a) **"Affiliate"** means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control", for purposes of this definition, means direct or indirect ownership or control of 50% or more of the voting interests of the subject entity.

(b) **"Authorized Affiliate"** means any of Customer's Affiliate(s) which is explicitly permitted to use the Services pursuant to the Agreement between Customer and Contentsquare but has not signed its own agreement with Contentsquare and is not a "Customer" as defined under the Agreement.

(c) "**CCPA"** means the California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et. seq.

(d) The terms, "**Controller**", "**Data Subject**", "**Member State**", "**Processor**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR. The terms "**Business**", "**Business Purpose**", "**Consumer**", "Sale", "Sell", "Selling", and "**Service Provider**" shall have the same meaning as in the CCPA.

(e) For the purpose of clarity, within this DPA "Controller" shall also mean "Business", and "Processor" shall also mean "Service Provider". In the same manner, Processor's Sub-processor shall also refer to the concept of Service Provider. "**Data Protection Laws**" means all privacy and data protection laws and regulations, including the GDPR, CCPA, 2018 Data Protection Act (UK GDPR) and any other laws and regulations of the European Union, the European Economic Area and their Member States, Switzerland, the United Kingdom and the United States of America, applicable to the Processing of Personal Data under the Agreement.

(f) **"Data Subject"** means the identified or identifiable person to whom the Personal Data relates.

(g) **"GDPR"** means the Regulation (EU) 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 and repealing Directive 95/46/EC (General Data Protection Regulation).

(h) **"Personal Data"** or **"Personal Information"** means any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, to or with an identified or identifiable natural person or Consumer (as defined in the CCPA), which is processed by Contentsquare solely on behalf of Customer, under this DPA and the Agreement between Customer and Contentsquare.

(i) **"Standard Contractual Clauses"** means the contractual clauses set out in Annex 2.

(j) **"Sub-processor"** means any third party that Processes Personal Data under the instruction or supervision of Contentsquare.

2. PROCESSING OF PERSONAL DATA

2.1 **Roles of the Parties.** The Parties acknowledge and agree that with regard to the Processing of Personal Data performed solely on behalf of Customer; (i) Customer is the Controller of its Users' Account Data and Profile Data, and of Customer Data (as defined in the Agreement), (ii) Contentsquare is the Processor of Customer Data, and of such Users' Account Data and Profile Data; (iii) for the purposes of the CCPA (and to the extent applicable), Customer is the "Business" and Contentsquare is the "Service Provider" (as such terms are defined in the CCPA), with respect to Processing of Personal Data described in this Section 2.1. The terms "**Controller**" and "**Processor**" signify Customer and Contentsquare, respectively.

2.2 **Customer's Processing of Personal Data.** Customer, in its use of the Services, and Customer's instructions to the Contentsquare, shall comply with the applicable Data Protection Laws. Customer shall establish and have any

and all required legal bases in order to collect, Process and transfer to Contentsquare the Personal Data, and to authorize the Processing by Contentsquare, and for Contentsquare's Processing activities on Customer's behalf, including the pursuit of 'business purposes' as under the CCPA (to the extent applicable). Customer shall publish and keep on Customer's site a privacy notice which accurately reflects and provide all required information under any applicable Data Protection Laws concerning the processing of personal data by Customer and Contentsquare under the Agreement. Customer shall obtain all consent required, under any applicable Data Protection Laws, by visitors to its websites and/or apps, and will maintain a record of such consents. It is agreed and acknowledged by Customer, that notwithstanding anything to the contrary under the Agreement, the services provided by Contentsquare under the Agreement are not intended for the processing of Personal Data other than Website/App Visitor Data (as defined under Annex 1 below). For such purpose, Customer shall restrict the transfer of any such excluded Personal Data to Contentsquare.

2.3 **Contentsquare's Processing of Personal Data.** When Processing solely on Customer's behalf under the Agreement, Contentsquare shall Process Personal Data for the following purposes: (i) Processing in accordance with the Agreement and this DPA; (ii) Processing for Customer to be able to use the Services; (iii) Processing to comply with Customer's reasonable and documented instructions, where such requests are consistent with the terms of the Agreement, regarding the manner in which the Processing shall be performed; (iv) rendering Personal Data fully anonymous, non-identifiable and non-personal; (v) Processing as required under any applicable Data Protection Laws to which Contentsquare is subject; in such a case, Contentsquare shall inform Customer of the legal requirement before Processing, unless that law prohibits such information on important grounds of public interest.

To the extent that Contentsquare cannot comply with an instruction from Customer, Contentsquare (i) shall inform Customer, providing relevant details of the problem, (ii) Contentsquare may, without any kind of liability to Customer, temporarily cease all Processing of the affected Personal Data (other than securely storing such data) and/or suspend access to the Account, and (iii) if the Parties do not agree on a resolution to the issue in question and the costs thereof, Customer may, as its sole remedy, terminate the Agreement and this DPA with respect to the affected Processing, and Customer shall pay to Contentsquare all the amounts owed to Contentsquare or due before the date of termination. Customer will have no further claims against Contentsquare (including, without limitation, requesting refunds for Services) pursuant to the termination of the Agreement and the DPA as described in this paragraph.

2.4 **Details of the Processing.** The subject-matter of Processing of Personal Data by Contentsquare is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Annex 1 (Details of the Processing) to this DPA.

2.5 **CCPA Standard of Care; No Sale of Personal Information**. Contentsquare acknowledges and confirms that it does not receive or process any Personal Information as consideration for any services or other items that Contentsquare provides to Customer under the Agreement. Contentsquare shall not have, derive, or exercise any rights or benefits regarding Personal Information Processed on Customer's behalf, and may use and disclose Personal Information solely for the purposes for which such Personal Information was provided to it, as stipulated in the Agreement and this DPA. Contentsquare represents and warrants that it understands the rules, requirements and definitions of the CCPA and agrees to refrain from selling (as such term is defined in the CCPA) any Personal Information Processed hereunder, without Customer's prior written consent, nor taking any action that would cause any transfer of Personal Information to or from Contentsquare under the Agreement or this DPA to qualify as "selling" such Personal Information under the CCPA.

3. RIGHTS OF DATA SUBJECTS

3.1 **Data Subject Requests.** Contentsquare shall, to the extent legally permitted, promptly notify Customer if Contentsquare receives a request from a Data Subject or Consumer to exercise their rights (to the extent available to them under applicable law) of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, its right not to be subject to an automated individual decision making, to opt-out of the sale of Personal Information, or the right not to be discriminated against for exercising any CCPA Consumer rights ("**Data Subject Request**"). Taking into account the nature of the Processing, Contentsquare shall assist Customer by appropriate technical and organizational measures, insofar as this is possible and reasonable, for the fulfillment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws. Contentsquare may refer Data Subject Requests received, and the Data Subjects making them, directly to the Customer for its treatment of such requests.

4. CONTENTSQUARE PERSONNEL

4.1 **Confidentiality.** Contentsquare shall ensure that its personnel engaged in the Processing of Personal Data have committed themselves to maintaining the confidentiality the Personal Data.

4.2 Without derogating from Section 2.3 above and Section 5 below, Contentsquare may disclose and Process the Personal Data after providing written notice to Customer: (a) to the extent required by a court of competent jurisdiction or other competent governmental or semi-governmental authority, or (b) otherwise as required by applicable Data Protection Laws (in such a case, Contentsquare shall inform the Customer of the legal requirement

before the disclosure, unless legally prohibited from doing so), or (c) on a "need-to-know" basis under an obligation of confidentiality to its legal counsel(s), data protection advisor(s) and accountant(s).

5. AUTHORIZATION REGARDING SUB-PROCESSORS

5.1 **Appointment of Sub-processors.** Customer acknowledges and agrees that: (a) Contentsquare's Affiliates may be retained as Sub-processors; and (b) Contentsquare and Contentsquare's Affiliates may each engage third-party Sub-processors in connection with the provision of the Services, all in accordance with and under the terms of this Section 5.

5.2 **Use of Sub-Processors**. Contentsquare makes available to Customer the current list of Sub-processors used by Contentsquare to process Personal Data at https://contentsquare.com/privacy-center/subprocessors/ ("Sub-Processor List"). The Sub-Processor List as of the date of first use of the Services by Customer is hereby authorized and in any event shall be deemed authorized by Customer unless it provides a written reasonable objection in accordance with the terms of Section 5.3 below within thirty (30) calendar days following the signing of this DPA. In order to receive notification concerning the intention of including a new Sub-Processor into the Sub-Processor List, please subscribe by sending an email to privacy@contentsquare.com of your request to receive notifications of any new Sub-processors used to Process Personal Data. Once subscribed, Contentsquare shall provide notification of any new Sub-processor(s) before authorizing such new Sub-processor(s) to Process Personal Data in connection with the provision of the Services.

5.3 **Objection Right.** Customer may reasonably object to Contentsquare's use of a new Sub-processor, for reasons relating to the protection of Personal Data intended to be Processed by such Sub-processor, by providing a written notice to Contentsquare at privacy@contentsquare.com, listing all specific legitimate gaps allegedly preventing the use of such Sub-processor by Contentsquare, within thirty (30) calendar days after receipt of Contentsquare's notice in accordance with the mechanism set out in Section 5.2 above. Failure to object to such new Sub-processor in writing within such time period shall be deemed as acceptance of the new Sub-Processor by Customer. In the event Customer reasonably objects to a new Sub-processor, as permitted in the preceding sentences, Contentsquare shall have the right to cure the objection through one of the following options (to be selected at Contentsquare's sole discretion): (i) Contentsquare shall cease to use the Sub-processor with regard to Customer Personal Data; (ii) Sub-processor shall take the corrective steps curing the gaps listed by Customer in its objection (which steps will be deemed to resolve Customer's objection) and proceed to use the Sub-processor to process Customer Personal Data; or (iii) Contentsquare may cease to provide, temporarily or permanently, the particular aspect of a Contentsquare Service that would involve use of the subcontractor to process Customer Personal Data ("**Objection Remediations**"). If Contentsquare is unable to implement any of the above Objection Remediations within thirty (30) calendar days of receipt of objection notice, Customer may, as a sole remedy, terminate the applicable Agreement and this DPA with respect only to those Services which cannot be provided by Contentsquare without the use of the objected-to Sub-processor. All amounts due under the Agreement before the termination date with respect to the Processing at issue shall be duly paid to Contentsquare. Until a decision is made regarding the new Sub-processor, Contentsquare may temporarily suspend the Processing of the affected Personal Data and/or suspend access to the Account. Customer will have no further claims against Contentsquare due to the use of approved Sub-processors in accordance with the terms of this Section 5 or termination or suspension of any part of the Contentsquare Service in accordance with the terms of this Section 5 or the termination of the Agreement (including, without limitation, requesting refunds) and/or the DPA in the situation described in this paragraph.

5.4 **Agreements with Sub-processors**. Contentsquare or a Contentsquare's Affiliate has entered into a written agreement with each Sub-processor containing appropriate safeguards to the protection of Personal Data. Where Contentsquare engages a new Sub-processor for carrying out specific Processing activities on behalf of the Customer, the same or materially similar data protection obligations as set out in this DPA shall be imposed on such new Sub-processor by way of a contract, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR. Where the new Sub-processor fails to fulfil its data protection obligations, Contentsquare shall remain fully responsible for and liable to the Customer for the performance of the new Sub-processor's obligations.

6. SECURITY

6.1 **Controls for the Protection of Personal Data.** Contentsquare shall maintain industry-standard technical and organizational measures for protection of Personal Data Processed hereunder (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data), confidentiality and integrity of Personal Data, including those measures set forth in the Security Documentation, as may be amended from time to time. Upon the Customer's reasonable request, Contentsquare will assist Customer, at Customer's cost, in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR taking into account the nature of the processing and the information available to Data Contentsquare.

6.2 **Third-Party Certifications and Audits.** Each calendar year, Contentsquare shall engage an appropriately recognized accreditor to conduct an audit in accordance with ISO 27001, or other similarly recognized standards (a "**Data Protection Controls Audit**"). Contentsquare shall cooperate with Customer and, upon reasonable prior notice to Contentsquare (no less than thirty (30) days), provided that Customer agrees to our Penetration Testing Protocol, Customer may conduct periodic technical security tests (manual penetration tests) and audits of

Contentsquare's systems holding or containing any Customer Personal Data, using a third party provider (under confidentiality obligations no less strict than the obligations of Customer under this Agreement), to verify that all necessary security measures have been implemented and are functioning properly, and in any event no more than once per each calendar year (a "**Technology Security Audit**"). Arising deficiencies and their associated criticality should be reviewed and mutually agreed on by both Parties Contentsquare shall promptly address all critical deficiencies, concerns or recommendations arising out of any Security Questionnaire, Data Protection Controls Audit, or Technology Security Audit (each a "**Security Audit**"). If, as a result of any Security Audit, Customer reasonably deem Contentsquare's security measures insufficient, then promptly following Customer's written request, a senior Contentsquare executive shall meet with a representative of Customer to discuss the matter in good faith until its conclusion. Notwithstanding the foregoing, all assessments and audits conducted under this Section 7.2 shall conform to the following requirements: (i) 30 days prior written notice; (ii) limited to once every twelve months; (iii) at the sole cost of the Customer; (iv) scope of assessments and audits shall be limited to matters not covered by the SOC 2 or ISO 27001 certifications in effect; and (v) any internal expenses incurred by Contentsquare as part of assessments and audits requested by the Customer with a scope already covered by the SOC 2 or ISO 27001 certifications in effect, shall be reimbursed by the Customer.

7. PERSONAL DATA INCIDENT MANAGEMENT AND NOTIFICATION

Contentsquare maintains security incident management policies and procedures and, to the extent required under applicable Data Protection Laws, shall notify Customer's notification email address (as informed by Customer to Contentsquare) without undue delay (no later than forty-eight (48) hours) after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data Processed on behalf of the Customer, including Personal Data transmitted, stored or otherwise Processed by Contentsquare or its Sub-processors of which Contentsquare becomes aware (a "**Personal Data Incident**"). Contentsquare shall make reasonable efforts to identify the cause of such Personal Data Incident and take those steps as Contentsquare deems necessary and reasonable in order to remediate the cause of such a Personal Data Incident to the extent the remediation is within Contentsquare's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or Customer's users.

Customer's notification email: _____. Customer may inform Contentsquare of changes to such notification email by emailing privacy@contentsquare.com.

8. RETURN AND DELETION OF PERSONAL DATA

Upon termination of the Agreement and subject thereto, Contentsquare shall, at the choice of Customer (indicated through the Service or in written notification to Contentsquare), delete or return to Customer all the Personal Data it Processes solely on behalf of the Customer in the manner described in the Agreement, and Contentsquare shall delete existing copies of such Personal Data unless Data Protection Laws require the storage of the Personal Data.

9. CROSS-BORDER DATA TRANSFERS

9.1 **Transfer of Personal Data from the EEA or United Kingdom.** Contentsquare may Process Personal Data from the EEA (as defined below) and/or the United Kingdom in such country outside EEA and the United Kingdom as provided in the Sub-Processor List. Customer hereby approves the transfer of Personal Data to the locations stated in the Sub-Processor List.

9.2 **Transfers from the EEA or United Kingdom to countries that offer adequate level or data protection**. Personal Data may be transferred from EU Member States, the three EEA member countries (Norway, Liechtenstein and Iceland) (collectively, "**EEA**") or United Kingdom to countries that offer an adequate level of data protection under or pursuant to the adequacy decisions published by the relevant data protection authorities of the EEA, the European Union, the United Kingdom, the Member States or the European Commission ("**Adequacy Decisions**"), without any further safeguard being necessary.

9.3 **Transfers Personal Data from the EEA or United Kingdom to the United States or other countries or entities**. If the Processing of Personal Data includes transfers (either directly or via onward transfer) from the EEA or United Kingdom to the United States or other countries which have not been subject to an Adequacy Decision ("Other Countries"), and such transfer or disclosure is not permitted through alternative means approved applicable Data Protection Laws, Contentsquare will take all reasonable steps to ensure that personal data is treated securely and in accordance with applicable Data Protection Laws, including by signing of a data transfer agreement governed by the Standard Contractual Clauses. Where the transfer of Personal Data is made subject to the Standard Contractual Clause, the "Data Importer" thereunder shall be either the Contentsquare or Sub-Processor, as the case may be and as determined by Contentsquare, and the "Data Exporter" shall be the Controller of such Personal Data. If necessary, Contentsquare will ensure that its Sub-processor enters into Standard Contractual Clauses with Customer directly, and Customer hereby gives Contentsquare an instruction and mandate to sign the Standard Contractual Clauses with any such Sub-processor in Customer's name and on behalf of Customer.

10. AUTHORIZED AFFILIATES

10.1 **Contractual Relationship.** The Parties acknowledge and agree that, by executing the DPA, the Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, in which case each Authorized Affiliate agrees to be bound by the Customer's obligations under this DPA, if and to the

extent that Customer Processes Personal Data on the behalf of such Authorized Affiliates, thus qualifying them as the "Controller". All access to and use of the Services by Authorized Affiliates must comply with the terms and conditions of the Agreement and this DPA and any violation of the terms and conditions therein by an Authorized Affiliate shall be deemed a violation by Customer.

10.2 **Communication.** The Customer shall remain responsible for coordinating all communication with Contentsquare under the Agreement and this DPA and shall be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

11. DISCLOSURE TO THIRD PARTIES

Contentsquare shall notify Customer without undue delay and in any case within seven business days if it receives a request from any third party for disclosure of personal data processed under this DPA where compliance with such request is required or purported to be required by applicable law unless such notification is prohibited by applicable law. Contentsquare shall reject any requests for Personal Data disclosures that are not legally binding.

12. OTHER PROVISIONS

12.1 **Data Protection Impact Assessment.** Upon Customer's reasonable request, Contentsquare shall provide Customer, at Customer's cost, with reasonable cooperation and assistance needed to fulfil Customer's obligation under the GDPR (as applicable) to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Contentsquare. Contentsquare shall provide, at Customer's cost, reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this Section 12.1, to the extent required under the GDPR.

12.2 **Assistance.** In addition to other express obligations under this DPA, Contentsquare may assist Customer, at Customer's request and cost, in ensuring compliance with Customer's obligations pursuant to the GDPR, CCPA and other applicable Data Protection Laws.

12.3 **Modifications.** Customer may by at least forty-five (45) calendar days' prior written notice to Contentsquare, request in writing any variations to this DPA if they are required as a result of any change in, or decision of a competent authority under, any Data Protection Laws, to allow Processing of those Customer Personal Data to be made (or continue to be made) without breach of that Data Protection Law. If Customer gives notice with respect to its request to modify this DPA under this Section 12.3, then: (a) Contentsquare shall make commercially reasonable efforts to accommodate such modification request; and (b) Customer shall not unreasonably withhold or delay agreement to any consequential variations to this DPA proposed by Contentsquare to protect the Contentsquare against additional risks, or to indemnify and compensate Contentsquare for any further steps and costs associated with the variations made herein. If Customer gives notice under this Section 12.3, the Parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Customer's notice as soon as is reasonably practicable. In the event that the Parties are unable to reach such an agreement within thirty (30) days of Customer's notice, then Customer or Contentsquare may, by written notice to the other Party, with immediate effect, terminate the Agreement to the extent that it relates to the Services which are affected by the proposed variations (or lack thereof). Customer will have no further claims against Contentsquare (including, without limitation, requesting refunds for Services) pursuant to the termination of the Agreement and the DPA as described in this Section 12.3.

IN WITNESS WHEREOF, the Parties hereto have caused this Agreement to be duly executed as of the Effective Date.

CUSTOMER	**CONTENT SQUARE SAS**
_____	_____
(Signature)	*(Signature)*
Name: _____	**Name:** _____
(Printed Name)	*(Printed Name)*
Title: _____	**Title:** _____
Date: _____	**Date:** _____

ANNEX 1 - DETAILS OF THE PROCESSING

Nature and Purpose of Processing

1. Providing the Services to Customer;
2. Performing the Agreement, this DPA and/or other contracts executed by the Parties;
3. Acting upon Customer's instructions, where such instructions are consistent with the terms of the Agreement;
4. Providing support and technical maintenance, if agreed in the Agreement;
5. Preventing, mitigating and investigating the risks of data security incidents, fraud, error or any illegal or prohibited activity;
6. Resolving disputes;
7. Enforcing the Agreement, this DPA and/or defending Contentsquare's rights;
8. Complying with applicable laws and regulations; and
9. All tasks related with any of the above.

Duration of Processing

Subject to any Section of the DPA and/or the Agreement dealing with the duration of the Processing and the consequences of the expiration or termination thereof, Contentsquare will Process Personal Data pursuant to the DPA and Agreement for the duration of the Agreement, unless otherwise agreed upon in writing.

Type of Personal Data

1. Personal Information of Customer's website and mobile app visitors ("Website/App Visitor Data"), such as:
    a. Unique Identification Information (e.g., IP addresses, cookie ID's and other similar unique identifiers);
    b. Website and mobile app technical information (e.g., pages of a website or app a visitor visited, visitor's type of computer operating system, visitor's type of web browser, JS error, other backend technical data, etc.);
    c. Behavioral Information (e.g. how a visitor has interacted with the website or app, mouse or touch movements, scrolls, mouse clicks, screen taps or zoom information; time of engagement, etc.).
    d. Additional visitor personal information as may be agreed by the parties.

2. Personal Data submitted by the Customer via the Services, the extent of which is determined and controlled by Customer in its sole discretion.

Categories of Data Subjects

Customer may submit Personal Data to the Services which may include, but is not limited to, Personal Data relating to the following categories of Data Subjects:

- Customer's website and mobile app visitors
- Employees, agents, advisors, freelancers of Customer (who are natural persons)
- Prospects, customers, business partners and vendors of Customer (who are natural persons)
- Employees or contact persons of Customer's prospects, customers, business partners and vendors
- Any other third-party individual with whom Customer decides to communicate through the Services

ANNEX 2 - STANDARD CONTRACTUAL CLAUSES

These Clauses are deemed to be amended from time to time, to reflect any change (including any replacement) made in accordance with those Data Protection Laws (i) by the European Commission to or of the equivalent contractual clauses approved by the European Commission under the GDPR (in the case of the Data Protection Laws of the European Union or a Member State); or (ii) by an equivalent competent authority to or of any equivalent contractual clauses approved by it or by another competent authority under another Data Protection Law (otherwise).

If these Clauses are not governed by the law of a Member State, the terms "Member State" and "State" are replaced, throughout, by the word "jurisdiction".

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: …
Address: …
Tel. …; fax …; e-mail: …
Other information needed to identify the organisation
…
(the data exporter)

And

Name of the data importing organisation: **Content Square SAS**
Address: **5 boulevard de la Madeleine, Paris 75001, France**
Tel. **+33 (0)1 83 75 88 00**; fax N/A; e-mail: **privacy@contentsquare.com**
Other information needed to identify the organisation: N/A
…
(the data importer)

each a ‘party’; together ‘the parties’,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
(d) that it will promptly notify the data exporter about:
  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
  (ii) any accidental or unauthorised access, and
  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;
(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.
   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.
3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full): …
Position: …
Address: …
Other information necessary in order for the contract to be binding (if any): …

Signature…….

On behalf of the data importer:

Name (written out in full): **Arnaud Gouachon**
Position: **Chief Legal Officer**
Address: **One Penn Plaza, Suite 5415, New York, NY, 10119 United States**
Other information necessary in order for the contract to be binding (if any): **N/A**

Signature…….

APPENDIX 1

TO THE 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:

The entity described as Customer under the Data Processing Agreement signed by the parties

Data importer
The data importer is:

Content Square SAS

Data subjects
The personal data transferred concern the following categories of data subjects:

Data Exporter may submit Personal Data through the Data Importer services which may include, but is not limited to, Personal Data relating to the following categories of Data Subjects:

- Data Exporter's website and mobile app visitors
- Employees, agents, advisors, freelancers of Data Exporter (who are natural persons)
- Prospects, customers, business partners and vendors of Data Exporter (who are natural persons)
- Employees or contact persons of Data Exporter's prospects, customers, business partners and vendors
- Any other third-party individual with whom Data Exporter decides to communicate through the Data Importer services

Categories of data
The personal data transferred concern the following categories of data:

1. Personal Information of Data Exporter's website and mobile app visitors, such as:
    a. Unique Identification Information (e.g., IP addresses, cookie ID's and other similar unique identifiers);
    b. Website and mobile app technical information (e.g., pages of a website or app a visitor visited, visitor's type of computer operating system, visitor's type of web browser, JS error, other backend technical data, etc.);
    c. Behavioral Information (e.g. how a visitor has interacted with the website or app, mouse or touch movements, scrolls, mouse clicks, screen taps or zoom information; time of engagement, etc.).
    d. Additional visitor personal information as may be agreed by the parties.

2. Personal Data submitted by the Data Exporter via the Data Importer services, the extent of which is determined and controlled by Data Exporter in its sole discretion.

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data:

It is not intended for the Data Exporter to transfer any special categories of personal data to Data Importer, as Data Importer contractually restricts the transfer of any special categories of personal data and provides Data Exporter with the tools necessary to block any transfer of such categories of data when using the Data Importer services.

Processing operations
The personal data transferred will be subject to the following basic processing activities:

Collection, transfer, recording, organisation, structuring, storage, deletion, aggregation, analyzation, anonymization and pseudonymization in order to provide analysis services of website and app visitor behaviour.

DATA EXPORTER

Name:……
Authorised Signature ……

DATA IMPORTER

Name: **Content Square SAS**
Authorised Signature ……

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):

1. Contentsquare designates a fully qualified employee to coordinate with Customer and provide to Customer, as needed, all information reasonably requested in writing by Customer concerning the processing, storage and protection of Customer Data.

2. Contentsquare has implemented and maintains a written data information security program for the protection of Customer Data that included appropriate organizational, administrative, technical and physical safeguards and other security measures that are industry standard and commensurate with the nature of the Customer Data processed by Contentsquare (the "Information Security Program"). Contentsquare's Information Security Program includes regular training of its personnel on those policies, hiring and exit procedures including regular risk assessment of the risks to the security of Customer Data, and shall be updated as necessary with changes in any applicable law. Contentsquare reserves the right to and may update or modify such measures from time to time provided that such updates or modifications do not result in any material degradation to the security of Customer Data.

3. Contentsquare implements appropriate physical, technical and organizational measures to ensure a level of security appropriate to the risk presented by processing Customer Data, in particular from unlawful and unauthorized destruction, loss, disclosure, or access to Customer Data, stored or otherwise processed by Contentsquare ("Security Breach"), including, inter alia, as appropriate: (i) implementation of reasonable and sufficient physical barriers and controls to prevent unauthorized physical access to, or compromise of Customer Data by human or environmental causes; (ii) ensuring that only those authorized Contentsquare representatives gain access to the Customer Data, and taking commercially reasonable steps to prevent unauthorized access to or destruction or loss of any Customer Data; and, (iii) maintaining a secure processing environment for Customer Data, which includes: (a) timely application of anti-virus updates, system patches, fixes and updates to all operating systems and applications, the implementation of firewalls and other similar measures designed to ensure the confidentiality, integrity, and availability of Customer Data; (b) encryption of all Customer Data at all times in transit and at rest, using and deploying a commercially acceptable encryption solution; and, (c) secure email for all Contentsquare domains; provided that the security contact provided by Customer is relevant, valid and up to date at the time of said Incident.

4. Contentsquare maintains a business continuity plan so that Customer Data is protected and in the event of a disruption to, or loss of data or CS Solution, delivery of CS Solution and access to Customer Data are restored and continue at the applicable service levels. The plan is being reviewed and approved by management level and tested periodically.

5. If at any time Contentsquare determines that any individual or entity has attempted to circumvent or has circumvented the security of any computer, system, or device containing Customer Data, or that there has been a Security Breach (each, an "Incident"), Contentsquare shall: (a) immediately terminate any unauthorized access and within forty-eight (48) hours notify Customer in writing of such Incident; (b) promptly investigate and take reasonable steps to remediate the Incident; and (c) cooperate with Customer investigation and provide documentation and assistance as may reasonably be requested by Customer.

6. Each calendar year, Contentsquare shall engage an appropriately recognized accreditor to conduct an audit in accordance with ISO 27001, or other similarly recognized standards ("Data Protection Controls Audit"). Contentsquare shall cooperate with Customer and, upon reasonable prior notice to Contentsquare (no less than thirty (30) days), provided that Customer agrees to our Penetration Testing Protocol, Customer may conduct periodic technical security tests (manual penetration tests) and audits of Contentsquare's systems holding or containing any Customer Data, using a third party provider (under confidentiality obligations no less strict than the obligations of Customer under this Agreement), to verify that all necessary security measures have been implemented and are functioning properly, and in any event no more than once per each calendar year (a "Technology Security Audit"). Arising deficiencies and their associated criticality should be reviewed and mutually agreed on by both Parties Contentsquare shall promptly address all critical deficiencies, concerns or recommendations arising out of any Security Questionnaire, Data Protection Controls Audit, or Technology Security Audit (each a "Security Audit"). If, as a result of any Security Audit, Customer reasonably deem Contentsquare's security measures insufficient, then promptly following Customer's written request, a senior Contentsquare executive shall meet with a representative of Customer to discuss the matter in good faith until its conclusion. Notwithstanding the foregoing, all assessments and audits conducted under Section 6 above shall conform to the following requirements: (i) 30 days prior written notice; (ii) Limited to once every twelve months; (iii) At the sole cost of the Customer; (iv) Scope of assessments and audits shall be limited to matters not covered by the SOC 2 or ISO 27001 certifications in effect; and (v) Any internal expenses incurred by Contentsquare as part of assessments and audits requested by the Customer with a scope already covered by the SOC 2 or ISO 27001 certifications in effect, shall be reimbursed by the Customer.