DATA PROTECTION ADDENDUM
(EU Standard Contractual Clauses)

This Data Protection Addendum ("**DPA**") effective this [⬛⬛⬛⬛⬛⬛⬛⬛⬛] ("**DPA Effective Date**") executed by and between Campaign Monitor Pty Ltd on behalf of itself and any Affiliates that are providing services to the Customer (collectively for the purposes of this DPA and except where otherwise indicated, "**Campaign Monitor**") and the Customer forms a part of the Terms of Use Agreement located at www.campaignmonitor.com/policies (or if Customer and Campaign Monitor execute a written agreement for use of the Services, then this DPA forms a part of that executed agreement)(the "**Agreement**") and reflects the parties' agreement with respect to the Processing of Personal Data in accordance with the requirements of Data Protection Laws. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

In the course of providing the Campaign Monitor Services to Customer pursuant to the Agreement, Campaign Monitor may Process Personal Data on behalf of Customer. Campaign Monitor agrees to comply with the following provisions with respect to any Personal Data submitted by or for Customer to the Campaign Monitor Services or collected and Processed by or for Customer using the Campaign Monitor Services.

1. DEFINITIONS

"**Affiliate**" means an entity that directly or indirectly Controls, is Controlled by or is under common Control with an entity. "Control" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question. The term "Controlled" shall be construed accordingly.

"**Customer**" means the party to the Agreement that receives the Campaign Monitor Services.

"**Customer Data**" means any data that Customer and/or its End Client (where applicable) submits or provides to the Campaign Monitor Services.

"**Data Controller**" means the entity which determines the purposes and means of the Processing of Personal Data.

"**Data Processor**" means the entity which Processes Personal Data on behalf of the Data Controller.

"**Data Protection Law(s)**" means all laws and regulations applicable to the Processing of Personal Data under the Agreement, including EU Data Protection Law and any laws pertaining to spam (including but not limited to, the U.S CAN-SPAM Act of 2003, Canadian CASL).

"**Data Subject**" means the individual to whom Personal Data relates.

"**EU Data Protection Law**" means (i) prior to 25 May 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of Personal Data and on the free movement of such data ("**Directive**"), respectively (ii) on and after 25 May 2018, Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation) ("**GDPR**"), and (iii) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) ("**e-Privacy Directive**"), as well as any national implementations of such laws (as may be amended, superseded or replaced).

"**Personal Data**" means any information relating to an identified or identifiable natural person to the extent such information is protected as personal data under applicable Data Protection Laws and is submitted as Customer Data.

"**Process**" or "**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"**Sub-processor**" means any Data Processor engaged by Campaign Monitor or a Campaign Monitor Affiliate to Process Personal Data in connection with the Services. Sub-processors may include third parties or Campaign Monitor Affiliates.

"**Security Breach**" means any unauthorized or unlawful breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Personal Data Processed by Campaign Monitor and/or its Sub-processors.

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, Customer and/or End Client (as applicable) is the Data Controller and Campaign Monitor is a Data Processor and that Campaign Monitor may engage Sub-processors pursuant to the requirements set forth in Section 6 ("Sub-processors") below.

2.2   **Details of the Processing.** The subject matter of the Processing under this DPA is Personal Data. As between Customer and Campaign Monitor, the duration of the Processing under this DPA is for the duration of the Agreement and for such period of time thereafter until Customer requests deletion of all of Customer's Data, including Personal Data. The purposes and nature of the Processing are described in the Agreement and this DPA or as otherwise agreed by the parties in writing. The types of Personal Data and categories of Data Subjects are specified in Attachment 1 (Appendix 1 to the Standard Contractual Clauses).

2.3   **Customer's Processing of Personal Data.** Customer agrees that: (i) it shall (and shall procure each End Client) comply with its obligations as a Data Controller under Data Protection Laws in respect of the Processing of Personal Data and any Processing instructions it issues to Campaign Monitor; and (ii) it has provided (and shall procure all End Clients provide) all notices and obtained (or will obtain) all consents and rights necessary for Campaign Monitor to Process Personal Data pursuant to the Agreement and this DPA in accordance with the requirements of applicable Data Protection Law. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer and/or its End Client (as applicable) acquired Personal Data. Without prejudice to the generality of the foregoing, Customer agrees that it shall be responsible for complying with (and procuring all End Clients comply with) all laws (including applicable Data Protection Laws) applicable to its emails, including those relating to acquiring consents (where required) to send emails, the content of the emails and its email deployment practices.

2.4   **Campaign Monitor's Processing of Personal Data.** As a Data Processor, Campaign Monitor shall only Process Personal Data for the purposes of providing the Campaign Monitor Services on behalf of and in accordance with Customer's documented lawful instructions. For these purposes, Customer instructs Campaign Monitor to Process Personal Data for the following purposes: (i) Processing in accordance with Appendix 1 of Standard Contractual Clauses in Attachment 1; (ii) Processing to perform the Campaign Monitor Services in accordance with the Agreement and this DPA; (iii) Processing initiated by any Users in their use of the Services; (iv) Processing to perform any steps necessary for the performance of the Agreement and this DPA; and/or (v) Processing to comply with other reasonable instructions provided by Customer (e.g., via email) provided such instructions are consistent with the terms of the Agreement and this DPA (collectively, the "**Instructions**"). The parties agree that the Instructions are the Customer's complete and final instructions to Campaign Monitor in relation to Processing of Personal Data. Processing outside the scope of Instructions (if any) will require prior written agreement between Campaign Monitor and Customer (each acting reasonably) on additional instructions for Processing, including agreement on any additional fees Customer will pay to Campaign Monitor for carrying out such instructions.

2.5   **Tracking Technologies**. Customer acknowledges that in connection with the performance, optimization and performance of the Services, Campaign Monitor and/or its third party data partners may use cookies, tags, we beacons, pixels and/or similar tracking technologies ("**Cookies**"). Customer shall (and shall procure that all End Clients) maintain appropriate notice and consent mechanisms as required by applicable Data Protection Laws (or a reasonably requested by Campaign Monitor) and industry best practice to enable Campaign Monitor and its third party data partners to deploy Cookies lawfully on, and collect data from, the devices of Subscribers and Users for the purposes of providing the Services. Campaign Monitor shall provide Customer with all information reasonably requested by the Customer (including details about the Cookies) to enable Customer and where applicable, its End Clients, to provide such notice, provided that Customer understands that any assistance, including any suggested language or methods offered by Campaign Monitor shall not constitute legal advice or a substitute for legal advice. Customer shall promptly notify Campaign Monitor if it is unable to comply with its obligations under this Section 2.5.

2.6   **Campaign Monitor Data**. Notwithstanding anything to the contrary in the Agreement (including this DPA), Customer acknowledges that Campaign Monitor shall have a right to use and disclose data relating to the operation, performance, support and/or use of the Campaign Monitor Services for its own legitimate business purposes, such as billing, account management, compliance with anti-spam laws, technical support and to improve and develop the Services. To the extent any such data is considered personal data under applicable Data Protection Laws, Campaign Monitor shall: (i) process such data in accordance with the Campaign Monitor's online privacy

policy, the most current version of which is available here: https://www.campaignmonitor.com/policies/#privacy-policy (as updated from time to time) and applicable Data Protection Laws; and (ii) ensure that, to the extent possible, the data is effectively anonymized, pseudonymized and/or aggregated data so that it does not reveal the specific identity of any individual. Subject to complying with this Section 2.6, nothing in the Agreement (including this DPA) shall prevent or restrict Campaign Monitor from using or sharing any such data.

3.   COOPERATION

3.1   **Correction, Blocking and Deletion.** To the extent Customer, in its use of the Campaign Monitor Services, does not have the ability to correct, amend, block or delete Personal Data, as required by Data Protection Laws, Campaign Monitor shall (at Customer's expense) comply with any commercially reasonable request by Customer to facilitate such actions to the extent Campaign Monitor is legally permitted to do so.

3.2   **Data Subject Requests.** Campaign Monitor shall, to the extent legally permitted, and in so far as it is possible to identify the Customer as the Controller of the data, promptly notify Customer if it receives a request from a Data Subject seeking to exercise the following Data Subject rights: access, rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, objection to the Processing, or to not be subject to automated individual decision making (each a "**Data Subject Request'**). Taking into account the nature of the Processing, Campaign Monitor shall assist Customer by appropriate technical and organizational measures, in so far as this is possible, for the fulfilment of the Customer's obligations to respond to a Data Subject Requests under applicable Data Protection Laws. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Campaign Monitor shall upon Customer's request provide reasonable co-operation to assist Customer to respond to any such Data Subject Requests, to the extent Campaign Monitor is required under applicable Data Protection Laws. To the extent legally permitted, Customer shall be responsible for any costs arising from Campaign Monitor's provision of such assistance, including any fees associated with provision of additional functionality. In the event any Data Subject Request is made directly to Campaign Monitor, Campaign Monitor shall not respond to such communication directly without Customer's prior authorization (except to guide the Data Subject to reach out to Customer), unless legally compelled to do so. If Campaign Monitor is required to respond to such request, Campaign Monitor will promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so.

3.3   If Campaign Monitor is required to respond to a subpoena, court order, warrant, audit or agency action and that occurrence demands that Campaign Monitor discloses any Personal Data, Campaign Monitor will promptly notify the Customer and provide Customer with a copy of the demand, unless legally prohibited from doing so.

3.4   **Data Protection Impact Assessments**. To the extent Campaign Monitor is required under Data Protection Laws, Campaign Monitor will (at Customer's expense) provide reasonably requested information regarding the Campaign Monitor Services to enable the Customer to carry out data protection impact assessments and prior consultations with data protection authorities as required by law.

4.   SECURITY MEASURES AND DATA BREACH RESPONSE

4.1   **Security Measures.** Campaign Monitor will implement and maintain appropriate technical and organizational security measures to protect Personal Data from Security Breaches and to preserve the security and confidentiality of the Personal Data ("**Security Measures**"). The security measures applicable to the Campaign Monitor Services are set forth in Appendix 2 of the Standard Contractual Clauses attached at Attachment 1, as updated or replaced from time to time in accordance with Section 4.2.

4.2   **Updates to Security Measures.** Customer acknowledges that the Security Measures are subject to technical progress and development and that Campaign Monitor may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Campaign Monitor Services.

4.3   **Personnel.** Campaign Monitor shall take commercially reasonable steps to ensure the reliability of any Campaign Monitor personnel engaged in the Processing of Personal Data, including ensuring that any person who is authorized by Campaign Monitor to Process Personal Data (i) will Process Personal Data in accordance with this DPA and (ii) has committed themselves to confidentiality or under an appropriate statutory obligation of confidentiality.

4.4   **Security Breach Response.** Upon becoming aware of a confirmed Security Breach, Campaign Monitor will notify Customer without undue delay after becoming aware of a confirmed Security Breach and will provide all

assistance and information relating to the Security Breach as it becomes known or as is reasonably requested by Customer. Campaign Monitor will use reasonable endeavors to mitigate and, where possible, to remedy the effect of, any Security Breach in accordance with the Security Measures. Where required by applicable Data Protection Laws, Campaign Monitor shall document the Security Breach and the facts surrounding it, the effects and any remedial action taken.

4.5   **Customer Responsibilities.** Notwithstanding the above, Customer agrees that except as provided by this DPA, Customer is responsible for its secure use of the Services, including securing its account authentication credentials, protecting the security of Customer Data when in transit to and from the Services and taking any appropriate steps to protect account passwords and/or backup any Customer Data uploaded to the Services.

5.   AUDITS

5.1   Upon Customer's request, Campaign Monitor will provide Customer with copies of any of Campaign Monitor's relevant audit report summaries and/or certifications and/or responses to questionnaires as reasonably required by Customer to verify Campaign Monitor's compliance with Article 28 of the GDPR ("**Audit Information**"). Customer agrees to leverage existing documentation provided by Campaign Monitor to the extent such documentation satisfies the requirements of Article 28 of the GDPR. The Customer acknowledges that the Audit Information constitutes Campaign Monitor's confidential information and it will protect such information in accordance with confidentiality provisions of the Agreement. Campaign Monitor shall further provide written responses to all reasonable requests for information made by Customer related to data protection that Customer may have in connection with the Audit Information.

6.   SUBPROCESSORS

6.1   **Authorized Sub-processors**. Customer agrees that in connection with the provision of the Campaign Monitor Services, Campaign Monitor may appoint Sub-processors to process Personal Data under the Agreement. The Sub-processors currently engaged by Campaign Monitor and authorized by Customer are listed in Attachment 2 of this DPA. Campaign Monitor shall provide via email or reasonable means an updated version of this list upon written request by Customer.

6.2   **Sub-processor Obligations.** Where Customer authorizes any Sub-processor, Campaign Monitor shall: (i) ensure that any such Sub-processor's will be obliged to protect the Personal Data in to the same standard provided for by this DPA, to the extent applicable to the nature of the services provided by the Sub-processor; (ii) remain responsible for any acts or omissions of the Sub-processor that cause Campaign Monitor to breach any of its obligations under this DPA to the same extent as it is liable under the Agreement.

6.3   **Changes to Sub-Processors.**

6.3.1   **Notification.** Beginning May 25, 2018, Customer may receive notifications of new Sub-processors by subscribing to notifications here: https://www.campaignmonitor.com/notifications/sub-processors/ after executing this DPA. If Customer subscribes, Campaign Monitor shall provide the subscriber with e-mail notification of new Sub-processor(s). Note that the process for Sub-processor updates notification may be modified in the future in Campaign Monitor's reasonable discretion.

6.3.2   **Objection.** Customer may reasonably object to Campaign Monitor's use of a new Sub-processor (e.g., if making Personal Data available to the Sub-processor may violate applicable Data Protection Law or weaken the protections for such Personal Data) by notifying Campaign Monitor in writing within ten (10) business days after receipt of Campaign Monitor's e-mail notice (as set out in Section 6.3.1 above). Such notice shall explain the reasonable grounds for the objection. In the event Customer objects to a new Sub-processor, as permitted in the preceding sentence, Campaign Monitor will use commercially reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Customer. If Campaign Monitor is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, either party may terminate without penalty the applicable Order Form(s) with respect only to those Services which cannot be provided by Campaign Monitor without the use of the objected-to new Sub-processor by providing written notice to Campaign Monitor.

7.   INTERNATIONAL TRANSFERS

7.1   **Processing Locations**. Subject to complying with this Section 7, Customer agrees that Campaign Monitor may transfer (directly or via onward transfer) and Process Personal Data to the United States, Australia and anywhere else in the world where Campaign Monitor, its Affiliates or its Sub-processors maintain data processing

operations. Campaign Monitor shall at all times ensure appropriate safeguards to protect the Personal Data processed, in accordance with the requirements of applicable Data Protection Laws

7.2   EU **Data Transfers.** To the extent that Campaign Monitor transfers (directly or via onward transfer) and Processes Personal Data that is subject to Data Protection Laws of the European Union, European Economic Area (EEA) and/or their member states, Switzerland and/or United Kingdom (for the purposes of this DPA, the "EU"), in or to ay recipient or country: (i) not deemed to provide an adequate safeguards (within the meaning of applicable Data Protection Law) for any such Personal Data, Customer and Campaign Monitor acknowledge and agree that the Standard Contractual Clauses (for Processors) in Attachment 1 ("Standard Contractual Clauses") and the additional terms set out in Attachment 3 will apply to the Processing of Personal Data by Campaign Monitor. For the purposes of the Standard Contractual Clauses, Campaign Monitor agrees that it is a "data importer" and Customer is the "data exporter" (notwithstanding that Customer may be an entity located out the EU).

7.3   **Alternative Transfer Mechanism.** The parties agree that the data export solution identified in this Section 7 shall not apply if and to the extent that Campaign Monitor adopts an alternative data export solution for the lawful transfer of Personal Data (as recognized under applicable Data Prsotection Law) outside of the EU ("**Alternative Transfer Mechanism**"), in which event, the Alternative Transfer Mechanism shall apply instead (but only to the extent such Alternative Transfer Mechanism extends to the territories to which Personal Data is transferred).

8.   **GENERAL PROVISIONS**

8.1   **Termination.** This DPA and the Standard Contractual Clauses will terminate simultaneously and automatically with the termination or expiry of the Agreement.

8.2   **Return or deletion of data.** Upon termination or expiration of the Agreement, Campaign Monitor shall (at Customer's election) delete or return to Customer all Personal Data (including copies) in its possession or control, save that this requirement shall not apply to the extent Campaign Monitor is required by applicable law to retain some or all of the Personal Data, or to Personal Data that Campaign Monitor is a Controller of.

8.3   **Limitation of Liability.** For the avoidance of doubt, any claim or remedies the Customer may have against Campaign Monitor, any of Campaign Monitor Affiliates and their respective employees, agents and sub-processors arising under or in connection with this DPA, including: (i) for breach of this DPA; (ii) as a result of fines (administrative, regulatory or otherwise) imposed upon Customer; (iii) under applicable Data Protection Laws, including any claims relating to damages paid to a data subject; and (iv) breach of its obligations under any associated Standard Contractual Clauses, will be subject to any limitation and exclusion of liability provisions (including any agreed aggregate financial cap) that apply under the Agreement. Notwithstanding this, the Customer's maximum recovery arising out of any claim against Campaign Monitor, Campaign Monitor Affiliates and their respective employees, agents and Sub-processors for any losses howsoever caused by Campaign Monitor shall be limited to Campaign Monitor's recovery from that third party Sub-processor where such recovery is less than the maximum aggregate liability set out in the Agreement.

8.4   **Governing Law and Jurisdiction.** This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, except to the extent that applicable Data Protection Law and/or Standard Contractual Clauses require otherwise, in which event this DPA and/or Standard Contractual Clauses (as applicable) will be governed in accordance with applicable Data Protection Law and be subject to the jurisdiction of the relevant Data Controller (or data exporter in the case of the Standard Contractual Clauses).
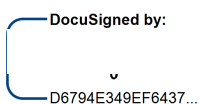
8.5   **Conflict.** In the event of any conflict or inconsistency between this DPA and the Standard Contractual Clauses in Attachment 1, the Standard Contractual Clauses shall prevail.

IN WITNESS WHEREOF, the parties hereto have executed the Agreement as indicated below.

Campaign Monitor Pty Ltd: **Customer (Company Legal Name):**

[   ]

Signature: Signature:

Name: Herry Wiputra   Name:

Title: CIO   Title:

Name: Herry Wiputra

Title: CIO

ATTACHMENT 1
STANDARD CONTRACTUAL CLAUSES

Commission Decision C(2010)593
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:

The entity identified as the data exporter the appendices of these Standard Contractual Clauses

(the data **exporter**)

And

Campaign Monitor Pty Ltd (ABN 42 094 533 445) established in Australia

(the d**ata 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[1];

(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

---

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

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[2]

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

---

[2]   Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia,* internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

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[3]. 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.

---

[3]   This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

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 1.

Data exporter: The data exporter is the company signing these Clauses and identified as the "Customer" in the Data Protection Addendum to which these clauses are appended (**"DPA"**). The data exporter will transfer personal data to Campaign Monitor in accordance with these Clauses in connection with the use of the Campaign Monitor's Services (defined below).

Data importer: The data importer is the Australian company Campaign Monitor Pty Ltd, acting on behalf of itself and its Affiliates to the extent they receive and process Personal Data (as defined in the DPA). The data importer provides cloud marketing software, for customer relationship management activities and the sending of email marketing communications ("**Services**").

Data subjects: Data exporter may submit personal data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include following categories of data subjects (past, present and future):
- Any person accessing and/or using the Service through data exporter and/or data exporter's end clients account ("**User**');
- Any individual: (i) whose email address is included in the Customer's Subscriber List; (ii) whose information is stored on or collected via the Services, or (iii) to whom Users send emails or otherwise engage or communicate with via the Services (collectively, "**Subscribers**").

Categories of data: Data exporter may submit personal data to the Campaign Monitor Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to the following categories of personal data:

- Customer and Users: identification and contact data (name, address, title, contact details, username); financial information (credit card details, account details, payment information); employment details (employer, job title, geographic location, area of responsibility);

- Subscribers: identification and contact data (name, date of birth, gender, general, occupation or other demographic information, address, title, contact details, including email address), personal interests or preferences (including purchase history, marketing preferences and publically available social media profile information); IT information (IP addresses, usage data, cookies data, online navigation data, location data, browser data); financial information (credit card details, account details, payment information).

Special categories of data (if appropriate): None. Data exporter agrees not to provide any personal data which falls into the Special Categories of personal data (e.g. any personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or any data concerning health or sex life).

Processing operations: The personal data transferred will be subject to the following basic processing activities:
- personal data storage, record keeping [and back-up]
- storage and other processing necessary to provide, maintain and improve the Services provided to data exporter;
- security scans and audits;
- to provide customer and technical support to data exporter;
- permission and compliance checks to avoid abuse

Duration of Processing: The duration of processing shall be for the term designated under the applicable DPA.

Scope and Purpose of Data Processing. The scope and purpose of processing personal data is described in the DPA.

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):

Campaign Monitor will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of personal data uploaded to the Campaign Monitor Services, as described on Campaign Monitor's Security Page: https://www.campaignmonitor.com/trust/security/.

On behalf of the data exporter: (Company Legal Name): [   ]
Name (written out in full): [   ]
Position: [   ]
Address: [   ]
Other information necessary in order for the contract to be binding (if any):

Signature……………………………………….

(stamp of organisation)

On behalf of the data importer: Campaign Monitor Pty Ltd
Name (written out in full): [Herry Wiputra   ]
Position: [CIO   ]
Address: Level 38, 201 Elizabeth Street, Sydney NSW 2000, Australia.

DocuSigned by:

Signature……..   …….

(stamp of organisation)

ATTACHMENT 2

LIST OF CURRENT SUB-PROCESSORS (LAST UPDATED 05/10/2018)

Customer Data (List of third party service providers, "Sub-processors", that process personal data of Customers)	- Internal Communication/Collaboration - Google G Suite - Slack - Billing/Invoicing/Payment - PayPal - NetSuite - Stripe (Payment/Collections) - User Support/Communication - Olark (In-app Support Communication) - Intercom (In-app communication) - TalkDesk (Sales Call Center) - Atlassian (Ticketing and Productivity Suite) - Citrix SendFile (Secure File Sharing) - Solvvy (Support Resource Management) - Livesize (Virtual Meetings) - GoToMeeting (Virtual Meeting) - Zoom (Virtual Meetings) - Droplr (Support Screen Shots) - Sprout Social (Social Media Support) - Dropbox (File Sharing) - Litmus (Email Testing) - Email on Acid (Email Testing) - User Analytics/Tracking - Gravatar - Mixpanel - MaxMind - DeviceAtlas (Device Identification) - HotJar (User Testing) - UserVoice (User Feedback) - Operations/Management - Groove App (Salesforce Sync) - Salesforce (CRM) - Aha! (Project Management) - Basecamp (Project Management) - Docusign (Contract Management) - Evernote (Project Management) - SnapLogic (Data Analytics) - DB Visualizer (Data Analytics) - Security - Splunk (Security Monitoring) - E-Hawk LLC (Anti-abuse/Security Measures) - SiftScience (Anti-abuse/Security Measures)
Subscriber Personal Data Subprocessing (List of third party service providers, "Sub-processors", that process personal data of Customer Subscribers)	- Security: - Splunk (Security Monitoring) - Amazon Web Services (Software Infrastructure) - User Support/Communication - TalkDesk (Support ticketing software) - Salesforce (Customer support case tracking) - Citrix SendFile (Secure File Sharing) - Dropbox (File Sharing) - Droplr (Support Screen Shots) - Internal Communication/Collaboration - Google G Suite - Slack

17

	- Atlassian (Ticketing and Productivity Suite) - Data Analytics: - SnapLogic (Data Analytics) - DB Visualizer (Data Analytics)
Other Third Parties (Name, purpose of processing, type of personal data processed by any other parties/systems)	Beaufort12 (CM4SFDC provisioning, Customer's Name, Company Name, email address, product's price and contract terms)

18

ATTACHMENT 3

ADDITIONAL TERMS TO STANDARD CONTRACTUAL CLAUSES

1. References in this Attachment 3 to (i) "data importer" and "data exporter" shall have the meanings given to them in the Standard Contractual Clauses; and (ii) "Clause" and "Clauses" shall mean clause and clauses in the Standard Contractual Clauses.

2. **Clause 4(h) and Clause 8: Disclosure of the Standard Contractual Clauses**. Data exporter agrees that the Standard Contractual Clauses constitute data importer's Confidential Information as that term is defined in the Agreement and may not be disclosed by data exporter to any third party without data importer's prior written consent unless permitted pursuant to the Agreement. This shall not prevent disclosure of these Clauses to a data subject pursuant to Clause 4(h) or a supervisory authority pursuant to Clause 8.

3. **Clause 5(a): Suspension of data transfers and termination.** For the purposes of Clause 5(a) of Standard Contractual Clauses, the parties agree that the Instructions (as defined in Section 2.4. of this DPA) set out data exporter's complete and final instructions to data importer for the Processing of Personal Data. The parties acknowledge that if data importer cannot provide such compliance for whatever reason, 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 Personal Data and/or terminate the Agreement. If the data exporter intends to suspend the transfer of Personal Data and/or terminate the Standard Contractual Clauses, it shall endeavor to provide notice to the data importer and provide data importer with a reasonable period of time to cure the non-compliance ("**Cure Period**"). If after the Cure Period the data importer has not or cannot cure the non-compliance then the data exporter may suspend or terminate the transfer of Personal Data immediately. The data exporter shall not be required to provide such Cure Period in instance where it considers there is a material risk of harm to data subjects or their Personal Data.

4. **Clause 5(f): Audit.** The parties agree that Section 5 of this DPA governing audit rights under the DPA, shall also govern the Customer's audit rights under the Standard Contractual Clauses. In the event that Customer wishes to exercise its audit rights under Standard Contractual Clauses (including under Clause 5(f) and Clause 12(2)), then Section 5 of this DPA shall exclusively govern the parties' obligations with respect to such audits.

5. **Clause 5(h) and Clause 11: Onward sub-processing.** Data exporter provides a general consent to data importer, pursuant to Clause 11, to engage onward Sub-processors. Such consent is conditional on data importer's compliance with Section 6 of this DPA, which collectively ensure that the onward Sub-processor will provide adequate protection for the Personal Data that it Processes.

6. **Clause 5(j): Disclosure of Sub-Processor Agreement.** The parties agree that at data exporter's reasonable written request, Campaign Monitor shall promptly provide copies of the sub-processor agreements pursuant to Clause 5(j) of the Standard Contractual Clauses. The parties further acknowledge that, pursuant to the Sub-processor's confidentiality restrictions, data importer may be restricted from disclosing onward sub-processor agreement to data exporter. Notwithstanding this, data importer shall use reasonable efforts to require any Sub-processor to permit it to disclosure the relevant sub-processor agreement to data exporter. Data importer may remove or redact all commercial information, or clauses unrelated to the Standard Contractual Clauses or their equivalent.

7. **Clause 12(1).** The parties agree that in satisfaction of Clause 12(1), on the completion or termination of the Agreement, Campaign Monitor shall, upon Customer's written request, delete or return all Personal Data in accordance with Section 3.1 and Section 8.2 of this DPA. The parties further agree that the certification of deletion of Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by Campaign Monitor to Customer only upon Customer's request.

8. **No Variation.** Nothing in this DPA varies or modifies the Standard Contractual Clauses nor affects any supervisory authority's or data subject's rights under applicable Data Protection Laws. In the event of any conflict or inconsistency between the body of this DPA and any of its Attachments (not including the Standard Contractual Clauses) and the Standard Contractual Clauses in Attachment 1 the Standard Contractual Clauses shall prevail.