

ACTIVECAMPAIGN DATA PROCESSING ADDENDUM

THIS DATA PROCESSING ADDENDUM (the “**DPA**”) is entered into between ActiveCampaign, LLC, a Delaware limited liability company located at 1 North Dearborn St., Fifth Floor, Chicago, IL 60602 (“**ActiveCampaign**”) and sLogic B.V., on behalf of itself and its Affiliates (collectively, “**Partner**”).

RECITALS

- A. This DPA supplements the ActiveCampaign Branded Agency Partner Program Agreement located at <https://www.activecampaign.com/legal/agency-partner-agreement> or such successor URL as determined by ActiveCampaign in its sole discretion (the “**Agreement**”) with Partner governing the provision of Services and is dated as of the date of last signature of a party below, and is hereby incorporated by reference into the Agreement. All capitalized terms not otherwise defined in this DPA will have the meaning given to them in the Agreement.
- B. As part of its privacy policy and its contractual arrangements, Partner has provided certain assurances to its clients, contacts, partners and/or end-users (collectively, “**Clients**”) to ensure the appropriate protection of Personal Data when Partner engages third party Processors.
- C. The parties are entering into this DPA to ensure that the Processing by ActiveCampaign of Personal Data within the Services on behalf of Partner and/or Partner’s Clients is done in a manner compliant with Applicable Privacy Laws and its requirements regarding the collection, use and retention of Personal Data of Data Subjects. Except as modified below, the terms of the Agreement shall remain in full force and effect.

AGREEMENT

1. DEFINITIONS

- 1.1 “**ActiveCampaign Group**” means ActiveCampaign and its Affiliates.
- 1.2 “**Affiliate**” means, with respect to the identified party, any entity that is directly or indirectly controlled by, controlling or under common control with such party.
- 1.3 “**Applicable Privacy Laws**” means data protection and privacy laws and regulations applicable to the Processing of Personal Data under the Agreement, including, where applicable, the GDPR, the UK GDPR, the CCPA, the LGPD and the Australian Privacy Act.
- 1.4 “**Australian Privacy Act**” means the Privacy Act 1988 (Cth) of Australia.
- 1.5 “**Authorized Person**” means any employee, officer, partner, principal, contractor or Subprocessor of ActiveCampaign who has access to Personal Data.
- 1.6 “**CCPA**” means California Consumer Privacy Act of 2018.
- 1.7 “**Data Subject**” means an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity.

ActiveCampaign Data Processing Addendum

- 1.8 **“GDPR”** means 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 (General Data Protection Regulation).
- 1.9 **“LGPD”** means the Brazilian General Data Protection Law.
- 1.10 **“Personal Data”** means Contact Data relating to a Data Subject (including, for the avoidance of doubt, personally identifiable information) submitted or otherwise provided by Partner or its Clients through the Services.
- 1.11 **“Privacy Shield”** means the EU-US and Swiss-US Privacy Shield self-certification programs operated by the U.S. Department of Commerce and approved by the European Commission pursuant to Decision C(2016)4176 dated July 12, 2016 (as may be amended, superseded, or replaced) and the Federal Council of Switzerland, respectively.
- 1.12 **“Privacy Shield Principles”** means the Privacy Shield Framework Principles (as supplemented by the Supplemental Principles) contained in Annex II to the European Commission Decision of 12 July 2016 pursuant to the Directive, details of which can be found at www.privacyshield.gov/eu-us-framework.
- 1.13 **“Process”** or **“Processing”** means any operation or set of operations which is performed on Personal Data, whether or not by automated means, such as the access, collection, use, storage, disclosure, dissemination, combination, recording, organization, structuring, adaption, alteration, copying, transfer, retrieval, consultation, disposal, restriction, erasure and/or destruction of Personal Data.
- 1.14 **“Security Breach”** means a breach of security leading to any accidental or unlawful loss, destruction, alteration, or unauthorized Processing of Personal Data under ActiveCampaign’s possession or control, that is notifiable under Applicable Privacy Law.
- 1.15 **“Sensitive Data”** means any (i) bank, credit card or other financial account numbers or login credentials, (ii) social security, tax, driver’s license or other government-issued identification numbers, (iii) health information identifiable to a particular natural person; or (iv) any “special” or “sensitive” categories of data as those terms are defined according to the GDPR or any similar category under other Applicable Privacy Laws.
- 1.16 **“Services”** refers to the services and tools provided by ActiveCampaign as defined within the Agreement.
- 1.17 **“Standard Contractual Clauses”** means the Standard Contractual Clauses promulgated by the European Commission Decision 2021/914/EU, under Module Three (transfer processor to processor).
- 1.18 **“Subprocessor”** means any third party (including any ActiveCampaign Affiliate) engaged by ActiveCampaign to Process any Personal Data on behalf of Partner, ultimately on behalf of Partner’s Clients, for the purpose of fulfilling ActiveCampaign’s obligations with respect to the provision of the Services under the Agreement.
- 1.19 **“UK GDPR”** means GDPR as incorporated into United Kingdom law by the Data Protection 2018 and amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019.

- 1.20 **“Usage Data”** means usage data collected by ActiveCampaign relating to the use of the Services by Partner.
- 1.21 The terms **“Controller”**, **“Processor,”** **“Business”** and **“Service Provider”** have the meanings given to them (or their equivalent term) in Applicable Privacy Laws. If and to the extent that Applicable Privacy Laws do not define such terms, then the definitions given to them in the GDPR and the CCPA will apply.

2. PURPOSE; OWNERSHIP OF DATA

- 2.1 Partner and ActiveCampaign have entered into the Agreement pursuant to which Partner is granted access to the Services, including for the purposes permitted within the Agreement. In using the Services, Partner or its Clients may submit through the Services or otherwise provide ActiveCampaign with access to Personal Data, which ActiveCampaign will Process only on the documented instructions of Partner which are included within this Agreement, and as permitted under Applicable Privacy Laws. Partner hereby instructs ActiveCampaign to Process Personal Data and, in particular, transfer Personal Data to any country as reasonably necessary to the provision of the Services and consistent with the Agreement. In addition, ActiveCampaign will not: (i) collect, retain, use, or disclose Personal Data for any purpose other than as necessary for the specific purpose of performing the Services as described in the Agreement, including use of the Personal Data for a commercial purpose other than providing the Services; and (ii) sell the Personal Data.
- 2.2 As between the parties, all Personal Data Processed under the terms of this DPA and the Agreement shall remain the property of Partner. Partner will be solely responsible for the accuracy, quality, integrity, legality, reliability, and appropriateness of all Personal Data. Under no circumstances will any member of the ActiveCampaign Group act, or be deemed to act, as a “Controller” (or equivalent concept) of the Personal Data Processed within the Services under any Applicable Privacy Laws. Additionally, in its provision of the Services, ActiveCampaign may collect and Process Usage Data. Such Usage Data, except to the extent such Usage Data contains Personal Data Processed on behalf of Partner and/or Partner’s Clients, is and shall remain the property of ActiveCampaign.
- 2.3 The parties acknowledge and agree that, for the purposes of the Applicable Privacy Laws and this Agreement, Partner’s Clients shall be considered as Controllers and/or Businesses, Partner shall be considered a Processor and/or Service Provider, and ActiveCampaign shall be considered another Processor and/or Service Provider engaged by Partner to carry out specific processing activities for Partner’s Clients.
- 2.4 ActiveCampaign will inform Partner if, in its opinion, Partner’s Processing instructions infringe any Applicable Privacy Law; in such event, ActiveCampaign is entitled to refuse Processing of Personal Data that it believes to be in violation of any Applicable Privacy Law. Such notification will not constitute a general obligation on the part of ActiveCampaign to monitor or interpret the laws applicable to Partner, and such notification will not constitute legal advice to Partner.

3. SUBPROCESSING

- 3.1 Partner agrees and provides general authorization for ActiveCampaign to appoint Subprocessors to assist it in providing the Services by Processing Personal Data on behalf of Partner, ultimately on behalf of Partner’s Clients, provided that such Subprocessors agree to protect Personal Data to a standard consistent with the requirements of this DPA, including

ActiveCampaign Data Processing Addendum

by implementing and maintaining appropriate technical and organizational measures to protect the Personal Data they Process consistent with the Security Measures described in Section 5.

- 3.2 Where so stated by Applicable Privacy Law, ActiveCampaign remains fully liable for any breach of this DPA or the Agreement that is caused by an act, error or omission of such Subprocessor.
- 3.3 The list of Subprocessors used in the provision of the Services who may have access to or Process Personal Data received by ActiveCampaign from Partner or its Clients through the Services under the Agreement is available at <https://www.activecampaign.com/legal/subprocessors> (or such successor URL as determined by ActiveCampaign in its sole discretion) (the “**Subprocessor Webpage**”) and may be updated from time to time. Prior to the addition or replacement of any Subprocessors, ActiveCampaign shall provide notice to Partner, which may include by updating the Subprocessor Webpage. It is Partner’s responsibility to check this website for changes.
- 3.4 In the event that Partner objects to the Processing of its Personal Data by any newly appointed Subprocessor as described in Section 3.3, it shall inform ActiveCampaign in writing within 7 days after notice has been provided by ActiveCampaign. In the event that Partner objects on reasonable grounds relating to the protection of Personal Data, ActiveCampaign will either, at ActiveCampaign’s option, (a) work with Partner to address Partner’s reasonable objections and thereafter proceed to use the Subprocessor to perform such Processing; (b) instruct the Subprocessor to cease any further Processing of Partner’s Personal Data, which may result in new Services features enabled by the Subprocessor not being available to Partner; or (c) allow Partner to immediately terminate the Agreement in respect of those Services that cannot be provided without the Subprocessor.
- 3.5 Partner acknowledges that any third party services that may be linked to or used within the ActiveCampaign Services (“**Non-ActiveCampaign Services**”) are governed solely by the terms and conditions and privacy policies of such Non-ActiveCampaign Services, and ActiveCampaign does not endorse, is not responsible or liable for, and makes no representations as to any aspect of such Non-ActiveCampaign Services, including, without limitation, their content or the manner in which they handle Personal Data or any interaction between Partner and the provider of such Non-ActiveCampaign Services. ActiveCampaign is not liable for any damage or loss caused or alleged to be caused by or in connection with Partner’s enablement, access or use of any such Non-ActiveCampaign Services, or Partner’s reliance on the privacy practices, data security processes or other policies of such Non-ActiveCampaign Services. The providers of Non-ActiveCampaign Services shall not be deemed Subprocessors for any purpose under this Agreement.

4. COOPERATION

- 4.1 To the extent ActiveCampaign is required under Applicable Privacy Laws, ActiveCampaign shall reasonably cooperate with Partner, insofar as this is possible, to enable Partner (or its third party Controller) to respond to any requests, complaints or other communications from Data Subjects and regulatory or judicial bodies relating to the Processing of Personal Data under the Agreement, including requests from Data Subjects seeking to exercise their rights under Applicable Privacy Laws (a “**DSR**”). Partner shall be responsible for any costs arising from ActiveCampaign’s provision of such assistance. In the event that any such DSR, complaint or communication is made directly to ActiveCampaign, ActiveCampaign shall promptly pass such communication on to Partner and shall not respond to such communication without

Partner's express authorization, unless required to do so by Applicable Privacy Laws or as otherwise permitted under the Agreement. For the avoidance of doubt, the foregoing shall not prohibit ActiveCampaign from communicating with a Data Subject if it is not reasonably apparent on the face of the communication to which Partner of ActiveCampaign the DSR relates.

- 4.2 If ActiveCampaign receives a subpoena, court order, warrant or other legal demand from a third party (including law enforcement or other public or judicial authorities) seeking the disclosure of Personal Data, ActiveCampaign shall, to the extent permitted by applicable laws, notify Partner in writing of such request, and reasonably cooperate with Partner if it wishes to limit, challenge or protect against such disclosure, to the extent permitted by applicable laws.
- 4.3 To the extent ActiveCampaign is required under Applicable Privacy Laws, ActiveCampaign will assist Partner (or its third-party Controller) to conduct a data protection impact assessment and, where legally required, consult with applicable data protection authorities in respect of any proposed Processing activity that present a high risk to Data Subjects. Partner shall be responsible for any costs arising from ActiveCampaign's provision of such assistance.
- 4.4 If the Applicable Data Privacy Laws and corresponding obligations related to the Processing of Personal Data change, the parties shall discuss in good faith any necessary amendments.

5. DATA ACCESS & SECURITY MEASURES

- 5.1 ActiveCampaign shall require that any Authorized Person is subject to a strict duty of confidentiality (whether a contractual or statutory duty).
- 5.2 ActiveCampaign will implement and maintain appropriate technical and organizational security measures consistent with industry standards to preserve the security, availability, integrity and confidentiality of Personal Data ("**Security Measures**"), in accordance with its obligations under Applicable Privacy Law.
- 5.3 ActiveCampaign's Security Measures shall include (as applicable):
 - (a) the pseudonymization and encryption of Personal Data (including during transmission);
 - (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
 - (c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
 - (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing; and
 - (e) the ability to allow data portability and ensure erasure of Personal Data (including by Subprocessors)

6. SECURITY INCIDENTS

- 6.1 In the event of a Security Breach, ActiveCampaign shall inform Partner, and provide written details of the Security Breach, without undue delay and in accordance with the timeframe required of it under Applicable Privacy Laws.
- 6.2 Furthermore, in the event of a Security Breach, ActiveCampaign shall at Partner's cost:

ActiveCampaign Data Processing Addendum

- (a) provide timely information and cooperation as Partner may reasonably require to fulfil Partner's personal data breach notification obligations under Applicable Privacy Laws; and
 - (b) take such measures and actions as are appropriate to remedy or mitigate the effects of the Security Breach and shall keep Partner up-to-date about developments in connection with the Security Breach.
- 6.3 The decision whether to provide notification, public/regulatory communication or press release (each, a "**Notification**") concerning the Security Breach shall be solely at Partner's discretion, but the content of any Notification that names ActiveCampaign or from which ActiveCampaign's identity could reasonably be determined shall be subject to the prior approval of ActiveCampaign, which approval shall not be unreasonably withheld, conditioned or delayed, except as otherwise required by applicable laws and provided that conditioning of the Notification on ActiveCampaign's approval shall not prevent Partner from complying with Applicable Privacy Laws.

7. RECORDS AND AUDITS

- 7.1 ActiveCampaign will keep at its normal place of business records of its Processing of Personal Data.
- 7.2 To the extent ActiveCampaign is required under Applicable Privacy Laws, at Partner's reasonable request and with advance written notice, ActiveCampaign will make available to Partner such records and information as is necessary to demonstrate its compliance with this DPA and allow Partner or a mutually agreed-upon, independent third party to conduct an onsite audit to verify such compliance. Any such audit will be conducted (a) on reasonable advance written notice to ActiveCampaign; (b) no more than once per year; (c) during ActiveCampaign's standard business hours; and (d) in such a manner to minimize disruption to ActiveCampaign's operations. Any information provided by ActiveCampaign in connection with such audit or generated as a result of such audit must be protected as ActiveCampaign's Confidential Information subject to a separate non-disclosure agreement entered into between ActiveCampaign and the recipient of such information before such audit. To request an audit, Partner must submit a detailed audit plan at least 90 days in advance of the proposed audit date describing the proposed scope, duration, and start date of the audit, subject to mutual agreement between the parties. Partner will bear the costs of such audit.
- 7.3 The parties agree that audits conducted pursuant to this Section 7 will be scoped to only matters not reasonably covered by ActiveCampaign's latest available security package, which will include a copy of ActiveCampaign's SOC 2 Type 2 report and which ActiveCampaign will provide to Partner upon Partner's written request. Such security package will constitute ActiveCampaign's Confidential Information.

8. DATA TRANSFERS

- 8.1 If Personal Data that originates in the European Economic Area ("**EEA**"), the United Kingdom, or Switzerland is transferred to ActiveCampaign for Processing in a country not subject to an adequacy decision in accordance with Applicable Privacy Laws ("**Data Transfer**"), the parties will conduct such Data Transfer in accordance with this Section 8.
- 8.2 ActiveCampaign will provide an adequate level of protection for the Personal Data, wherever Processed, in accordance with the requirements of Applicable Privacy Laws. Partner

ActiveCampaign Data Processing Addendum

acknowledges that ActiveCampaign and its Subprocessors may maintain data processing operations in countries that are outside of the EEA, the United Kingdom, and Switzerland. As such, both ActiveCampaign and its Subprocessors may Process Personal Data in non-EEA, non-United Kingdom, and non-Swiss countries.

8.3 The parties agree that:

- (a) Any Data Transfer will be conducted pursuant to the Standard Contractual Clauses (which will be deemed executed only upon signature of this DPA and of the relevant portions of the Standard Contractual Clauses), and the following terms will apply:
 - (1) Partner will be referred to as the “data exporter” and ActiveCampaign will be referred to as the “data importer” in such clauses;
 - (2) details in Annex A of this DPA and the Subprocessor Webpage will be used to complete Annex I.B of the Standard Contractual Clauses;
 - (3) details in Section 5 of this DPA will be used to complete Annex II of the Standard Contractual Clauses;
 - (4) the optional Clause 7 (Docking Clause) will not be included in the New Standard Contractual Clauses; and
 - (5) if there is any conflict between this DPA or the Agreement and the Standard Contractual Clauses, the Standard Contractual Clauses will prevail.
- (b) ActiveCampaign will promptly notify Partner if it makes a determination that it can no longer meet its obligations under Section 8.3(a) above, and in such event, to work with Partner and promptly take all reasonable and appropriate steps to stop and remediate (if remediable) any Processing until such time as the Processing meets the level of protection as is required by Section 8.2 and promptly cease (and procure all Subprocessors promptly cease) Processing such Personal Data if in Partner’ sole discretion, Partner determines that ActiveCampaign has not or cannot correct any non-compliance with Section 8.2 above in accordance with Section 8.3(b) within a reasonable time frame.
- (c) Although ActiveCampaign does not rely on the Privacy Shield as a legal basis for transfers of Personal Data originating in the EEA, the United Kingdom or Switzerland in light of the judgment of the Court of Justice of the EU in Case C-311/18, if ActiveCampaign maintains an active certification under the Privacy Shield, then ActiveCampaign will provide at least the same level of protection to such Personal Data as is required by the Privacy Shield Principles, in conjunction with its own Privacy Shield certification.

8.4 ActiveCampaign acknowledges that Partner may disclose this DPA and any relevant privacy or data protection provisions of the Agreement to the US Department of Commerce, European Data Protection Authorities, or any other US or EU judicial or regulatory body with jurisdiction in respect of Applicable Privacy Laws (each, a “**Data Regulatory Authority**”) upon their request, provided that for the avoidance of doubt this DPA shall remain ActiveCampaign’s Confidential Information subject to the restrictions in the Agreement notwithstanding any requirement to share it with a Data Regulatory Authority.

9. WARRANTIES OF RESELLER

As part of Partner receiving the Services under the Agreement, Partner represents and warrants:

ActiveCampaign Data Processing Addendum

- (a) that the Processing of Personal Data, including the instructions to ActiveCampaign in accordance with this Agreement, are and shall continue to be in accordance with all the relevant provisions of the Applicable Privacy Laws, particularly with respect to the security, protection and disclosure of Personal Data;
- (b) that if Processing by ActiveCampaign involves any Sensitive Data, Partner has collected such Sensitive Data in accordance with Applicable Privacy Laws;
- (c) that Partner will inform its Data Subjects:
 - (1) about its use of Processors and Service Providers to Process their Personal Data, including ActiveCampaign; and
 - (2) that their Personal Data may be Processed outside of the EEA, the United Kingdom, or Switzerland;
- (d) that it shall respond in reasonable time and to the extent reasonably practicable to enquiries by Data Subjects regarding the Processing of their Personal Data by Partner, and to give appropriate instructions to ActiveCampaign in a timely manner;
- (e) that it shall respond in a reasonable time to enquiries from a supervisory authority or any other applicable data protection authority regarding the Processing of relevant Personal Data by Partner; and
- (f) that Partner is and will at all relevant times remain duly and effectively authorized to act on behalf of each of its Affiliates.

10. DELETION

Upon Partner's request or upon termination or expiry of the Agreement, ActiveCampaign shall destroy all Personal Data in its possession or control. This requirement shall not apply to the extent that ActiveCampaign is required by any applicable law to retain some or all of the Personal Data, in which event ActiveCampaign shall isolate and protect the Personal Data from any further Processing except to the extent required by such law.


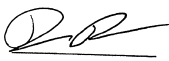
11. GENERAL

11.1 ACTIVECAMPAIGN MAKES NO REPRESENTATION OR WARRANTY THAT THIS DPA IS LEGALLY SUFFICIENT TO MEET PARTNER'S NEEDS UNDER APPLICABLE PRIVACY LAW, INCLUDING THE GDPR, UK GDPR, CCPA, LGPD AND AUSTRALIAN PRIVACY ACT. ACTIVECAMPAIGN EXPRESSLY DISCLAIMS ALL REPRESENTATIONS OR WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, THROUGH A COURSE OF DEALING, OR OTHERWISE THAT THIS DPA WILL COMPLY WITH OR SATISFY ANY OF PARTNER'S OBLIGATIONS UNDER APPLICABLE PRIVACY LAW, INCLUDING THE GDPR, UK GDPR, CCPA, LGPD AND AUSTRALIAN PRIVACY ACT. PARTNER FULLY UNDERSTANDS THAT IT IS SOLELY RESPONSIBLE FOR COMPLYING WITH ALL OF ITS OBLIGATIONS IMPOSED BY APPLICABLE PRIVACY LAW. THE PARTIES AGREE THAT THERE WILL BE NO PRESUMPTION THAT ANY AMBIGUITIES IN THIS DPA WILL BE CONSTRUED OR INTERPRETED AGAINST THE DRAFTER.

ActiveCampaign Data Processing Addendum

- 11.2 The parties acknowledge that the requirements of Applicable Privacy Laws differ between jurisdictions and, as such, certain of ActiveCampaign's obligations and responsibilities under this DPA will only apply where such obligations exist under Applicable Privacy Laws.
- 11.3 This DPA shall be effective on the date both parties sign this DPA and supersedes, replaces, and takes precedence over any other data processing addendum(s) executed by the same parties hereto, in their entirety, as of such effective date. The obligations placed upon the ActiveCampaign under this DPA shall survive so long as ActiveCampaign and/or its Subprocessors Processes Personal Data on behalf of Partner, ultimately on behalf of Partner's Clients, with the exception of confidentiality obligations on Authorized Persons which shall survive the termination of the Agreement.
- 11.4 This DPA may not be modified except by a subsequent written instrument signed by both parties.
- 11.5 If any part of this DPA is held unenforceable, the validity of all remaining parts will not be affected.
- 11.6 In the event of any conflict between this DPA and any Agreement, the parties agree that the terms of this DPA shall prevail, provided that each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA or any Agreement, whether in contract, tort or under any other theory of liability, shall remain subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and this DPA, including all Annexes hereto.

By signing below, each party acknowledges that it has read and understood the terms of this DPA and agrees to be bound by them.

sLogic B.V. By:  Name: <u>Jacob Schermers</u> Title: <u>Director</u> Date: 07 / 15 / 2022	ActiveCampaign, LLC By:  Name: Dawson Price Title: VP of Legal Date: 07 / 15 / 2022
---	--

ANNEX A

DETAILS OF THE PROCESSING

Nature and Purpose of Processing: ActiveCampaign specializes in the development of email marketing, marketing automation, sales, CRM, contact management, and business marketing services. Partner, uses and resells the Services in accordance with the Agreement to Process Personal Data of (1) its Clients, (2) such Clients' contacts, and (3) contacts for marketing and related customer relationship management purposes on a continuous basis. ActiveCampaign stores the Personal Data on its servers and Processes such Personal Data only for the purposes of, and in accordance with, the instructions of Partner and does not make any decisions itself as to the use, updating, or deletion of Personal Data.

Subject Matter of Processing: The context for the Processing of Personal Data is ActiveCampaign's provision of Services under the Agreement.

Duration of Processing: The Processing will begin on the effective date of the Agreement and will end upon expiration or termination of the Agreement.

Categories of Data Subjects: The Personal Data concern the following categories of Data Subjects: Customers and prospective customers of Partner and Partner's Clients and other marketing contacts determined by Partner in connection with Partner's use of the Services.

Categories of Personal Data: The Personal Data may concern the following categories of data, the extent of which is determined by Partner in its sole discretion: contact details including name, address, telephone or mobile number, fax number and email address; date of birth; personal bank account details; details of goods and/or services which customers/potential customer have purchased or inquired about; IP address; place of employment; occupation; personal interests; age; and other Personal Data collected and provided by Partner in connection with Partner's use of the Services.

Special categories of data (if appropriate): ActiveCampaign will not Process any Sensitive Data in its performance of the Services under the Agreement.

ANNEX B

STANDARD CONTRACTUAL CLAUSES (MODULE THREE)

SECTION I

Clause 1

Purpose and scope

- (a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) for the transfer of personal data to a third country.
- (b) The Parties:
 - (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and
 - (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

- (c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- (d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

- (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
- (b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

- (a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
 - (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
 - (ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
 - (iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
 - (iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
 - (v) Clause 13;
 - (vi) Clause 15.1(c), (d) and (e);
 - (vii) Clause 16(e);
 - (viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.
- (b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

- (a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- (c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional

Docking clause

Not Used.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE THREE: Transfer processor to processor

8.1 Instructions

- (a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.
- (b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.
- (c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.
- (d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I. B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary

to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a)

8.6 Security of processing

- (a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- (b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have

committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

- (c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
- (d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- (i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;
- (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

- (a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.
- (b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.
- (c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.
- (d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.
- (e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.
- (f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- (g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

MODULE THREE: Transfer processor to processor

- (a) **OPTION 2: GENERAL WRITTEN AUTHORISATION** The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 7 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).
- (b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree

that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

- (c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
- (d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
- (e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

MODULE THREE: Transfer processor to processor

- (a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.
- (b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
- (c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

Clause 11

Redress

- (a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

MODULE THREE: Transfer processor to processor

- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely

fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
 - (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
 - (ii) refer the dispute to the competent courts within the meaning of Clause 18.
- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

MODULE THREE: Transfer processor to processor

- (a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- (b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
- (c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
- (d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
- (e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

- (f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
- (g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

MODULE THREE: Transfer processor to processor

- (a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

- (b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE THREE: Transfer processor to processor

- (a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence

of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

- (b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
 - (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
 - (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
 - (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- (c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- (d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- (e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). The data exporter shall forward the notification to the controller.
- (f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation, if appropriate in consultation with the controller. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the controller or the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

MODULE THREE: Transfer processor to processor

15.1 Notification

- (a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
 - (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
 - (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

The data exporter shall forward the notification to the controller.

- (b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). The data exporter shall forward the information to the controller.
- (d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- (e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

- (a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not

disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

- (b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. The data exporter shall make the assessment available to the controller.
- (c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

- (a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
 - (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
 - (ii) the data importer is in substantial or persistent breach of these Clauses; or
 - (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority and the controller of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

- (d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure

compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

- (e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

MODULE THREE: Transfer processor to processor

OPTION 1: These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third- party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

MODULE THREE: Transfer processor to processor

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (b) The Parties agree that those shall be the courts of Ireland.
- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

ANNEX I

A. LIST OF PARTIES

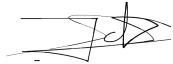
MODULE THREE: Transfer processor to processor

Data exporter:

Name: sLogic B.V.

Address: Vlasakkerweg 3B, Amersfoort, Utrecht, 3811 MR, Nederland

Activities relevant to the data transferred under these Clauses: The data exporter's use and resale of the Services under the Agreement

Authorized signature: 

Date: 07 / 15 / 2022

Signatory's name and position: Jacob Schermers, Director

Role (controller/processor): Processor

Contact person's name, position and contact details: Jacob Schermers, Director, jss@salesarchitects.nl

Data importer:

Name: ActiveCampaign, LLC

Address: 1 North Dearborn Street, Fifth Floor, Chicago, IL 60302

Activities relevant to the data transferred under these Clauses: The data importer's provision of the Services under the Agreement

Authorized signature: 

Date: 07 / 15 / 2022

Signatory's name and position: Dawson Price, VP of Legal

Role (controller/processor): Processor

Contact person's name, position and contact details: Legal Department, legal@activecampaign.com

B. DESCRIPTION OF TRANSFER

MODULE THREE: Transfer processor to processor

Please see details set forth in Annex A to the DPA and the Sub-processor Webpage.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE THREE: Transfer processor to processor

Identify the competent supervisory authority/ies in accordance with Clause 13

Where the data exporter is established in an EU Member State: The competent supervisory authority is the supervisory authority of the Member State in which the data exporter is established.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The competent supervisory authority is the supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The competent supervisory authority is the supervisory authority of the Member State in which the majority of data subjects whose personal data are processed are located.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE THREE: Transfer processor to processor

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Please see the Security Measures set forth in Section 5 of the DPA.

The data exporter acknowledges that the data importer is regularly audited by independent third party auditors for SOC 2 Type 2 compliance. The most recent certification is available upon request of the data exporter in accordance with Section 7.3 of the DPA.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

Where these Clauses apply pursuant to Section 8 of the DPA, then this Appendix 2 forms part of these Clauses and sets out the Parties' interpretations of their respective obligations under specific provisions within these Clauses, as identified below. Where a Party complies with the interpretations set out in this Appendix 2, that Party shall be deemed by the other Party to have complied with its commitments under these Clauses.

Nothing in the interpretations below is intended to vary or modify these Clauses or conflict with either Party's rights or responsibilities under these Clauses and, in the event of any conflict between the interpretations below and these Clauses, these Clauses shall prevail to the extent of such conflict. Notwithstanding this, the Parties expressly agree that any claims brought under these Clauses shall be exclusively governed by the limitations on liability set out in the Agreement. For the avoidance of any doubt, in no event shall any Party limit its liability with respect to any data subject rights under these Clauses.

Clause 8.3: Obligations of the data exporter regarding non-disclosure requirements

The data exporter agrees that the terms of these Clauses, as executed, constitute the data importer's Confidential Information and may not be disclosed by the data exporter to any third party without the data importer's prior agreement (other than to a data subject pursuant to Clause 8.3, with the exception of any business secrets or other confidential information, including the measures described in Annex II and personal data, as consistent with the Parties' obligations in that Clause).

Clause 8.9: Audits

Audits will be performed in accordance with Section 7 of the DPA.

Clause 9(a): Use of sub-processors

For the avoidance of any doubt, the data exporter acknowledges and expressly agrees to the data importer's engagement of subprocessors in accordance with Section 3 of the DPA. Such authorization is conditional on the data importer's compliance with the following requirements:

1. the data importer must restrict the sub-processor's access to personal data only to what is strictly necessary to perform its subcontracted data processing services to the data importer (which shall be consistent with the instructions issued to the data importer by the data exporter); and
2. the data importer will prohibit the subprocessor from processing the personal data for any other purpose.

Clause 9(c): Disclosure of sub-processor agreements

1. The Parties agree that the copies of the sub-processor agreements that must be provided by the data importer to the data exporter pursuant to Clause 9(c) may have all business secrets or other confidential information, or provisions unrelated to these Clauses, removed by the data importer beforehand and that such copies will be provided by the data importer, in a manner to be determined in its discretion, only upon request by the data exporter.
2. The Parties agree that all copies of the sub-processor agreements, and information related thereto, that the data importer provides to the data exporter will constitute the data

importer's Confidential Information and may not be disclosed by the data exporter to any third party without the data importer's prior agreement.

Clause 12: Liability

Any claims brought under these Clauses shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement in effect as of the date of execution of these Clauses or other written or electronic agreement for the data exporter's use and purchase of the data importer's products and services. In no event shall any Party limit its liability with respect to any data subject rights under these Clauses.

Clause 14(a): Supplementary Measures

1. The Parties acknowledge that it is the responsibility of the data exporter to verify whether the safeguards employed by the data importer are sufficient to meet its obligations under Applicable Law, including with respect to the provision of adequate safeguards necessary to secure the transfer of personal data through these Clauses.
2. The data importer has not, to its knowledge, received any requests for the personal data of EU residents processed within the provision of the Services, under Section 702 of the U.S. Foreign Intelligence Surveillance Act.
3. The Parties acknowledge that personal data transmitted between the data exporter and the data importer within the course of the Services is encrypted in transit.

Clauses 14(f), 16(b) and 16(c): Suspension of data transfers and termination

1. If the data exporter intends to suspend the transfer of personal data and/or terminate the contract, it shall endeavour to provide notice to the data importer and provide data importer with a reasonable period of time to cure the non-compliance ("Cure Period").
2. 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 notice in instance where it considers there is a material risk of harm to data subjects or their personal data.

Clauses 8.5 and 16(d): Obligation after the termination of personal data processing services

1. The data importer will fulfil its obligations pursuant to Clauses 8.5 and 16(d) by complying with Section 10 of the DPA.
2. Certification of deletion of personal data will be provided upon the data exporter's written request.

Replacement of the Old SCCs

If the Parties have executed the Standard Contractual Clauses (controller to processor) promulgated by the European Commission Decision 2010/87/EU ("Old SCCs"), then the Parties acknowledge and agree that these Clauses supersede and replace in their entirety the Old SCCs, which, as of the date of execution of these Clauses, will be terminated and have no further force or effect.

TITLE	Partner DPA (sLogic B.V. and ActiveCampaign)
FILE NAME	document_0
DOCUMENT ID	922ddc6957d9dae762285797e47efc9557a8f86e
AUDIT TRAIL DATE FORMAT	MM / DD / YYYY
STATUS	● Signed

Document History



SENT

05 / 13 / 2022

09:24:25 UTC-5

Sent for signature to Sales Architects (jss@salesarchitects.nl) and Rianne Chen (rchen@activecampaign.com) from rtucker@activecampaign.com
IP: 35.185.192.36



VIEWED

07 / 08 / 2022

05:19:02 UTC-5

Viewed by Sales Architects (jss@salesarchitects.nl)
IP: 80.73.246.124



SIGNED

07 / 15 / 2022

05:30:56 UTC-5

Signed by Sales Architects (jss@salesarchitects.nl)
IP: 80.73.246.124



VIEWED

07 / 15 / 2022

08:32:28 UTC-5

Viewed by Rianne Chen (rchen@activecampaign.com)
IP: 3.228.136.234



SIGNED

07 / 15 / 2022

08:33:45 UTC-5

Signed by Rianne Chen (rchen@activecampaign.com)
IP: 3.228.136.234



COMPLETED

07 / 15 / 2022

08:33:45 UTC-5

The document has been completed.