Updated May 2026

DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") is attached to and made a part of the Click Marketing Automation Terms of Service for the purchase of marketing automation services from ClickDimensions, LLC ("Click") (identified either as "**Services**" or otherwise in the applicable agreement, and hereinafter defined as "**Services**") (the "**Agreement**") to reflect the parties' agreement with regard to the Processing of Personal Data.

By signing the Agreement, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorized Affiliates, if and to the extent Click processes Personal Data for which such Authorized Affiliates qualify as the Controller. For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and Authorized Affiliates. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

In the course of providing the Services to Customer pursuant to the Agreement, Click may Process Personal Data on behalf of Customer and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

This DPA prevails over any additional, conflicting, or inconsistent terms and conditions appearing in the Agreement regarding the subject matter of this DPA. No other agreement may limit or extend the rights, obligations and/or liability of either Party under this DPA and under statutory law unless expressly agreed in this DPA or an amendment to this DPA.

DATA PROCESSING TERMS

1. DEFINITIONS

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

b) "**Authorized Affiliate**" means any of Customer's Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Customer and Click, but has not signed its own Order Form with Click and is not a "Customer" as defined under the Agreement.

c) **"Click"** means ClickDimensions, LLC, a company organized as limited liability company in the State of Georgia USA.

d) **"Click Group"** means ClickDimensions, LLC ("Click") and its Affiliates engaged in the Processing of Personal Data.

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

f) **"Customer Data"** means what is defined in the Agreement as "Customer Data".

g) **"Data Protection Laws and Regulations"** means all laws and regulations, including laws and regulations of (i) the European Union, the European Economic Area and their member states which implement the European Union Directive 95/46/EC and the Regulation 2016/679 (the ***"EU GDPR"***), Switzerland; and (ii) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**"); and (iii) the US Data Protection Laws, applicable to the Processing of Personal Data under the Agreement, in each case as amended, consolidated, re-enacted or replaced from time to time.

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

i) "**GDPR**" means collectively or as applicable, the EU GDPR and the UK GDPR.

j) **"Personal Data"** means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws and Regulations), where for each (i) or (ii), such data is Customer Data.

k) **"Processing"** means any operation or set of operations which is performed upon Personal Data, whether or not by automatic 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.

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

m) **"Regulator"** means the data protection supervisory authority which has jurisdiction over a Data Controller's Processing of Personal Data.

n) **"Security Documentation"** means the Security Documentation applicable to the specific Services purchased by Customer, as updated from time to time, and accessible via Click' webpage, or as otherwise made reasonably available by Click.

o) **"Standard Contractual Clauses"** or "**Clauses**" means (i) where the EU GDPR applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**EU SCCs**"); and (ii) where the UK GDPR applies, standard data protection clauses adopted pursuant to or permitted under Article 46 of the UK GDPR ("**UK SCCs**").

p) **"Sub-processor"** means any Processor engaged by Click or a member of the ClickDimesnions Group.

q) "**Supervisory Authority**" means an independent public authority which is established by an EU Member State pursuant to the GDPR.

r) **"Third Country"** means any country outside of the scope of the data protection laws of the European Union or the European Economic Area ***("EEA"),*** excluding countries recognized by the Regulator as providing adequate protection for Personal Data from time to time.

s) **"US Data Protection Laws"** means any relevant U.S. federal or state legal requirements, including the California Consumer Privacy Act of 2018, California Privacy Rights Act, Colorado Privacy Act, New York Stop Hacks and Improve Electronic Data Security ("SHIELD") Act, Utah Consumer Privacy Act, Washington Privacy Act, and Virginia Consumer Data Protection Act (as each is effective, and where applicable), and any implementing regulations, as amended, consolidated, re-enacted or replaced from time to time.

t) **"CCPA"** means the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq., including any amendments and any implementing regulations thereto that become effective on or after the effective date of this Data Processing Addendum.

Any terms not defined in this DPA but defined in the Data Protection Laws and Regulations shall have the meaning assigned to them in the Data Protection Laws and Regulations.

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 is the Controller, Click is the Processor and that Click or members of the Click Group will engage Sub-processors pursuant to the requirements set forth in Section 5 "Sub-processors" below.

2.2 **Customer's Processing of Personal Data.** Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the means by which Customer acquired Personal Data and for the accuracy, quality, and legality of Customer Data provided to Click within the framework of the Services. Customer is further responsible for determining the legal and regulatory status of Customer Data and ensuring that any Customer Data submitted to the Services complies with applicable laws and regulations and does not include data types that the Services are not designed to process. Customer acknowledges that its use of the Services will not knowingly or intentionally violate

the rights any Data Subject that has opted-out from sales or other disclosures of Personal Data, to the extent applicable under the applicable US Data Protection Laws.

2.3 **Click' Processing of Personal Data.** Subject to the terms of the Agreement, Click shall Process Personal Data in accordance with Customer's documented instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s); (ii) Processing for Customer to be able to use the Services; and (iii) Processing

to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement. To the extent that Click cannot comply with a change to Customer's instructions without incurring material additional costs and/or because in Click' reasonable opinion compliance with such instructions is legally prohibited or is likely to result in a violation of Data Protection Laws and Regulations, Click shall: (i) immediately inform Customer, giving full details of the problem; and (ii) cease all processing of the affected Personal Data (other than securely storing those data) until revised instructions are received. Any changes in Customer's instructions that affect the pricing structure or commercial relationship between the parties must go through an appropriate change control procedure.

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

3. RIGHTS OF DATA SUBJECTS

3.1 **Data Subject Requests**. Click shall, to the extent legally permitted, promptly notify Customer if Click receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making ("Data Subject Request"). Taking into account the nature of the Processing, Click shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Click shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Click is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for any costs arising from Click' provision of such assistance.

4. CLICK PERSONNEL

4.1 **Confidentiality.** Click shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. Click shall ensure that such confidentiality obligations survive the termination of the personnel engagement and/or the Agreement. Further details are provided in the Security Documentation.

4.2 **Reliability.** Click shall take commercially reasonable steps to ensure the reliability of any Click's personnel engaged in the Processing of Personal Data.

4.3 **Limitation of Access.** Click shall ensure that Click's access to Personal Data is limited to those personnel performing Services in accordance with the Agreement and only as required to perform the Services.

5. SUB-PROCESSORS

5.1 **Appointment of Sub-processors.** Customer acknowledges and agrees that Click may engage third-party Sub-processors in connection with the provision of the Services. Click has entered

into an agreement with each Sub-processor containing data protection obligations not less protective than those in this DPA with respect to the protection of Customer Data to the extent applicable to the nature of the Services provided by each such Sub-processor.

5.2 List of Current Sub-processors and Notification of New Sub-processors. The current list of Sub-processors used by Click is attached to this Addendum in Schedule 3 and also located here: https://support.clickdimensions.com/hc/en-us/sections/360009048952-Subprocessors?("**Sub-processor List**") and Customer consents to the use of such Subprocessors as of the date of this DPA. In addition, Customer hereby grants Click a general authorization to utilize new sub-processors in accordance with the process below. If Customer subscribes to the mechanism to subscribe to notifications of new Subprocessors, Click shall provide notification of a new Sub-processor(s) before authorizing

any new Sub-processor(s) to Process Personal Data in connection with the provision of the Services.

5.3 Objection Right for New Sub-processors. Customer may object to Click's use of a new Sub-processor by notifying Click promptly in writing within ten (10) business days after receipt of Click's notice in accordance with the mechanism set out in Section 5.2. In the event Customer objects to a new Sub-processor, as permitted in the preceding sentence, Click will use 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 the Customer. If Click is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer's sole remedy is to terminate the applicable Order Form(s) with respect only to those Services which cannot be provided by Click without the use of the objected-to new Sub-processor by providing written notice to Click.

5.4 Liability. Click shall be liable for the acts and omissions of its Sub-processors to the same extent Click would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

6. SECURITY; AUDIT

6.1 Controls for the Protection of Customer Data. Click shall maintain appropriate industry-standard technical and organizational measures for protection of the security

(including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer Data), confidentiality and integrity of Customer Data, including, as appropriate, the measures referred to in Article 32(1) of the GDPR and as set forth in the Security Documentation. Click regularly monitors compliance with these measures. Click will not materially decrease the overall security of the Services during a subscription term. **6.2 Third-Party Certifications and Audits.**

6.2.1 Upon Customer's request not more than once per year, and subject to the confidentiality obligations set forth in the Agreement, Click shall make available to Customer that is not a competitor of Click (or Customer's independent, thirdparty auditor that is not a competitor of Click) a copy of Click's then most recent third-party audits or certifications, as applicable. Notwithstanding the foregoing limitations, Customer may conduct an audit at any time in particular, if (i) a Customer Data Incident has occurred which concerns it; or (ii) an audit is formally requested by its data protection authority.

6.2.2 Upon Customer's request, Click will make available to Customer information necessary to demonstrate its compliance with the obligations set forth in this DPA.

Where the mandatory Data Protection Laws and Regulations provide Customer with a direct audit right, Click will allow for and operationally collaborate with audits, including inspections, conducted by Customer or another auditor designated by Customer (provided such an auditor is not a competitor of Click and has duly executed a non-disclosure agreement with Click). In case of such audit, Customer

may contact Click to request an on-site audit with at least sixty (60) days prior notice, which shall be limited to the audit of the architecture, systems and procedures relevant to the protection of Personal Data at Click's locations where Personal Data is stored. Before the commencement of any such on-site audit, Customer and Click shall mutually agree upon the scope, timing, and duration of the audit, none of which shall adversely impact Click's business activities. Customer shall promptly notify Click of any non-compliance discovered during the course of an audit. Customer shall bear the costs of all such audits, as well as of any follow-up requested by Customer to Click

7. CUSTOMER DATA INCIDENT MANAGEMENT AND NOTIFICATION

7.1.1 Click maintains security incident management policies and procedures specified in Security Documentation and, to the extent required under applicable Data Protection Laws and Regulations, shall notify Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data, including Personal Data, transmitted, stored or otherwise Processed by

Click or its Sub-processors of which Click becomes aware (a "**Customer Data Incident**"). Click shall make reasonable efforts to identify the cause of such Customer Data Incident and take those steps as Click deems necessary and reasonable in order to remediate the cause of such a Customer Data Incident to the extent the remediation is within Click's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or Customer's users.

7.1.2 In the event Click becomes aware of a Customer Data Incident, Click shall notify Customer by email, without undue delay (and in no event greater than 48 hours), after having become aware of the occurrence. Click will ensure that such notice complies with requirements under applicable Data Protection Laws and Regulations, including with respect to the timing and substance of such notice. Notwithstanding these requirements, such notification to Customer shall include: (i) a description of the nature of the Customer Data Incident, including, the categories and approximate number of Data Subjects concerned, the affected categories and approximate number of types of Processing of Personal Data; (ii) a description of the likely consequences of the Customer Data Incident; and (iii) a description of the measures taken or proposed to remedy the Customer Data Incident and, if necessary, the measures to mitigate or limit possible negative effects thereof. To the extent it is not possible to provide the foregoing information at the same time, the information may be provided in phases without further undue delay.

7.1.3 Taking into account the nature of Processing and the information available to Click, Click will provide assistance to Customer to enable Customer to fulfill its notification obligations to affected Data Subjects or relevant authorities in connection with a Customer Data Incident. At the written request of Customer, Click shall provide reasonable assistance to Customer and take such reasonable steps as requested by Customer agreed by the parties or necessary under Data Protection Laws and Regulations to assist in the investigation, remediation, and litigation of such Customer Data Incident. Customer shall be responsible for any reasonable costs arising from Click's provision of such assistance unless such Customer Data Incident is determined to have been caused by Click or its Sub-processors in which case Click shall provide such assistance without charge.

8. RETURN AND DELETION OF CUSTOMER DATA

Subject to the Agreement, Click shall, to the extent allowed by applicable law, delete Customer Data in accordance with the procedures and timeframes specified in applicable Data Protection Laws and Regulations.

Notwithstanding the foregoing, certain operational, security, audit, backup, deliverability, and service telemetry records maintained by Click or its authorized subprocessors may be retained for limited periods where reasonably necessary for security, fraud prevention, service integrity, troubleshooting, compliance, legal obligations, or operational continuity, subject to appropriate technical and organizational safeguards.

9. AUTHORIZED AFFILIATES

9.1 Contractual Relationship. The parties acknowledge and agree that, by executing the Agreement, the Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between Click and each such Authorized Affiliate subject to the provisions of the Agreement and this Section 9 and Section 10. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Agreement, and is only a party to the DPA. All access to and use of the Services by Authorized Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by Customer.

9.2 Communication. The Customer that is the contracting party to the Agreement shall remain responsible for coordinating all communication with Click under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

9.3 Rights of Authorized Affiliates. Where an Authorized Affiliate becomes a party to this DPA with Click, it shall, to the extent required under applicable Data Protection Laws and Regulations, be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

9.3.1 Except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against Click directly by itself, the parties agree that: (i) solely the Customer that

is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Authorized Affiliate individually but in a combined manner for all of its Authorized Affiliates together (as set forth, for example, in Section 9.3.2, below).

9.3.2 The parties agree that the Customer that is the contracting party to the Agreement shall, when carrying out an on-site audit of the procedures relevant to the protection of Personal Data, take all reasonable measures to limit any impact on Click and its Sub-Processors by combining, to the extent reasonable possible, several audit requests carried out on behalf of different Authorized Affiliates in one single audit.

10. LIMITATION OF LIABILITY

10.1 Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and Click, whether in contract, tort or under any other theory of liability, is 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 all DPAs together.

10.2 For the avoidance of doubt, Click and its Affiliates' total liability for all claims from the Customer and all of its Authorized Affiliates arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established under this Agreement, including by Customer and all Authorized Affiliates, and, in particular, shall not

be understood to apply individually and severally to Customer and/or to any Authorized Affiliate that is a contractual party to any such DPA.

10.3 Also for the avoidance of doubt, each reference to the DPA in this DPA means this DPA including its Schedules and Appendices (if any).

11. INTERNATIONAL TRANSFERS

11.1 EU GDPR. In relation to Personal Data that is protected by the EU GDPR, the EU SCCs are incorporated and will apply completed as follows: Module 2 of the EU SCCs applies between Customer as "data exporter" and Click as "data importer" on the following basis: (i) in Clause 7, the optional docking clause will apply, (ii) in Clause 9, Option 2 will apply, and the time period for prior notice of Sub-Processor changes shall be as set out in Section 11(c) of this Addendum, (iii) in Clause 11, the optional language shall not apply, (iv) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by _____, (v) in Clause 18(b), disputes shall be resolved before the courts of _____, (vi) Annex 1 to the EU SCCs will be deemed to incorporate Schedule 1 to this Addendum and (vii) Annex 2 to the EU SCCs will be deemed to incorporate Schedule 2 of this Addendum.

11.2 UK GDPR. In relation to Personal Data that is protected by the UK GDPR, UK Addendum to the EU Standard Contractual Clauses ("**UK Addendum**") issued by the Information Commissioner's Office (**"ICO"**) under s.119A(1) of the Data Protection Act 2018, Version B1.0, in force 21 March 2022, is hereby incorporated and will apply as follows: (i) the EU SCCs, completed as set out at Section 10(a) above shall also apply to transfers of such Personal Data, and (ii) the UK Addendum shall be deemed executed between Customer and Click, and the EU SCCs shall be deemed amended as specified by the UK Addendum in respect of the transfer of such Personal Data.

11.3 Data Protection Impact Assessment. Upon Customer's request, Click shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under the GDPR to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Click. Click shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to Section 11.1 of this DPA, to the extent required under the GDPR.

12. CCPA

For purposes of CCPA compliance, the Parties acknowledge and agree that the Service Provider will act as a "Service Provider" as that term is defined under the CCPA, in its performance of its obligations pursuant to the Main Agreement. The Customer will act as a single point of contact for its Affiliates with respect to CCPA compliance, such that if the Service Provider gives notice to the Customer, such information or notice will be deemed received by the Customer's Affiliates. The Parties acknowledge and agree that any claims in connection with the CCPA under this DPA will be brought by the Customer, whether acting for itself or on behalf of an Affiliate. The terms of this Section 12 are additional to the terms otherwise stated herein.

12.1.1 Instructions for CCPA Personal Information Processing

Insofar as Service Provider Processes Protected Data as defined in the CCPA on behalf of Customer, Service Provider shall not retain, use, or disclose Protected Data for any purpose other than for the limited and specific purpose of providing the Services, or as otherwise permitted by the CCPA. Service Provider acknowledges that it shall not retain, use, or disclose Protected Data for a commercial purpose other than providing the Services.

12.1.2 Processing Protected Data outside the scope of the DPA or the Main Agreement will require prior written agreement between Customer and Service Provider on additional instructions for Processing.

12.2 Required consents and notices

Where required by applicable laws, the Customer will ensure that it has obtained/will obtain all necessary consents, and has given/will give all necessary notices, for the Processing of Protected Data by the Service Provider in accordance with the Main Agreement.

12.3 Transfer of CCPA Personal Information

12.3.1 Service provider shall not disclose, release, transfer, make available, or otherwise communicate any Protected Data to another business or third party without the prior written consent of the Customer unless and to the extent that such disclosure is made to a Subprocessor for a business purpose, provider that the Service Provider has entered into a written agreement with Subprocessor which imposes the same obligations on the Subprocessor with regard to their Processing of Protected Data as are imposed on Service Provider under this DPA and the Main Agreement. Notwithstanding the foregoing, nothing in this Agreement shall restrict Service Provider's ability to disclose Protected Data to comply with applicable laws or as otherwise permitted by the CCPA.

12.3.2 Service Provider shall not sell any Protected Data to another business or third party without the prior written consent of Customer.

12.3.3 Service Provider shall comply with all applicable requirements of the CCPA and shall, where possible and reasonably practicable, assist Data Subject with responding to Data Subject Requests as required by applicable provisions of the CCPA.

12.3.4 Customer may take reasonable and appropriate steps to ensure that Service Provider's use of CCPA Personal Information is consistent with Customer's obligations under the CCPA with respect to the CCPA Personal Information.

12.3.5 Service Provider shall promptly notify Customer of any request received by the Service Provider from a Data Subject with respect to the Protected Data of the Data Subject, and shall direct the Data Subject to contact Customer. Customer is responsible for promptly responding to such requests within the timeframe prescribed by the CCPA.

12.3.6 Customer shall promptly notify Service Provider if Customer determines that it can no longer meet its obligations under the CCPA with respect to the CCPA Personal Information.

12.3.7 Upon receiving notice from Service Provider pursuant to Paragraph 1.5.6, Customer may take reasonable and appropriate steps to stop and remediate unauthorized use of CCPA Personal Information.

List of Schedules

- **SCHEDULE 1 – ANNEX 1 TO THE STANDARD CONTRACTUAL CLAUSES**
- **SCHEDULE 2 – ANNEX 2 TO THE STANDARD CONTRACTUAL CLAUSES**
- **SCHEDULE 3 – SUBPROCESSORS**

The parties' authorized signatories have duly executed this Agreement:

CUSTOMER:

Signature:

Customer Legal Name:

Print Name:

Title:

Date:

CLICKDIMENSIONS LLC :

Signature:

Legal Name: ClickDimensions LLC

Print Name:

Title:

Date:

SCHEDULE 1 – ANNEX 1 TO THE STANDARD CONTRACTUAL CLAUSES

A. **LIST OF PARTIES**

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1. Name: . . . . . .

. . . . . .

Address: . . . . . .

. . . .

Contact person's name, position and contact details: . . . . . .

. . . . . .

. . . . . .

Activities relevant to the data transferred under these Clauses: . . . . . .

. . . . . .

. . . . . .

Signature and date: . . . . . .

Role (controller/processor): . . . . . .

. . . . . .

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

1. Name: ClickDimensions, LLC

   Address: 5901 Peachtree Dunwoody Road, Suite C-370, Atlanta GA 30328

   Contact person's name, position and contact details: Fionnuala O'Donoghue, SVP, Finance, fionnuala.odonoghue@clickdimensions.com

   Activities relevant to the data transferred under these Clauses: Processing the data as necessary to provide the marketing automation services specified in the applicable order.

   Signature and date:

   Role: Processor.

B. **DESCRIPTION OF TRANSFER**

Categories of data subjects whose personal data is

transferred:

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

- Customer's users authorized by Customer to use the Services
- Employees, agents, advisors, freelancers of Customer (who are natural persons)
- Prospects, customers, business partners and vendors of Customer (who are natural persons)
- Employees or contact persons of Customer's prospects, customers, business partners and vendors

Categories of personal data transferred:

The specific data elements submitted and then processed by Click depends on which tools the Data Exporter uses and what fields are chosen to be included in emails, surveys, forms and profile management page. The data fields may include but are not limited to the following categories of Personal Data:

- Email address
- First and last name
- Title
- Phone number
- SMS data (Mobile Phone Number, Message Content)
- Information collected via forms and/or surveys (these fields are determined by the customer/data exporter and can range from Name and Email Address to free form text)
- Web-tracking information (IP Address, Page Visit and Page View data including timestamps, URLs, duration, Operating system, language and Linked Records, Page Title)

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose

limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures. None

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

The transfer will be on a continuous basis during the term of the applicable order.

Nature of the processing

The data will be processed as necessary to provide the email marketing automation services.

Purpose(s) of the data transfer and further processing

The data will be processed as necessary to provide the email marketing automation services.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

For the term of the services.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

See Annex III.

C. **COMPETENT SUPERVISORY AUTHORITY**

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

. . . . . .

SCHEDULE 2 – ANNEX 2 TO THE STANDARD CONTRACTUAL CLAUSES

ANNEX II

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

Click uses third party cloud providers to host applications and data. The certifications and controls of the cloud providers are reviewed on an annual basis including SOC 2 and ISO. Parts of the Physical Access and System Access Controls are managed by the cloud providers.

1. Confidentiality

- **Access control (Physical access)**
  No unauthorized access to data processing systems, e.g: Magnetic or chip cards, keys, electric door openers, factory security or gatekeepers, alarm systems, video systems;
-
  ☒ Alarm system
  ☒ Protection of building shafts
  ☒ Automatic access control system
  ☒ Chip card/transponder locking system
  ☒ Locking system with code lock
  ☒ Manual locking system
  ☒ Biometric access barriers
  ☒ Video surveillance of accesses
  ☒ Light barriers / motion detectors
  ☒ Safety locks
  ☒ Key regulation (key handout etc.)
  ☒ Visitor control at the porter's / reception desk
  ☒ Logging of visitors
  ☒ Careful selection of cleaning personnel
  ☒ Careful selection of security personnel
  ☒ Obligation to wear authorisation cards

- **Access control (Logical / System based access)**
  No unauthorized use of the system, e.g.: (Secure) passwords, automatic locking mechanisms, two-factor authentication, disk encryption;

  ☒ Assignment of user rights
  ☒ Creating user profiles
  ☒ Assignment of credentials (Password, Username)
  ☒ Authentication with username + strong password
  ☒ Assignment of user profiles to IT systems
  ☒ Use of VPN technology
  ☒ Use of intrusion detection systems
  ☒ Use of anti-malware software on Servers

☒ Use of anti-malware software on Endpoint Devices
☒ Encryption of hard disks on Endpoint Devices
☒ Use of a software firewalls

- **Access control (Organisational)**
  No unauthorized reading, copying, modifying or removing within the system, e.g: Authorization concepts and demand-oriented access rights, logging of accesses;

  ☒ Using an Authorization Concept
  ☒ Administration of access rights and user lifecycle management by system administrators ☒ Multifactor Authentication

☒ Number of administrators reduced to the "bare minimum”
☒ Password policy incl. password length, password expiration
☒ Secure storage of data storage devices
☒ Physical deletion of data media before reuse
☒ Irrecoverable destruction of data storage devices
☒ Use of document shredders or service providers (if possible, with data protection seal of approval)
☒ Encryption of data storage devices
☒ Encryption of data in transit using TLS protocols and latest Strong Ciphers

- **Separation control**
  Separate processing of data collected for different purposes, e.g. multi-client capability, sandboxing;

☒ Physically separate storage on separate systems or data storage devices
☒ Logical client separation (software-based)
☒ Creation of an authorization concept
☒ Encryption of data sets processed for the same purpose
☒ Providing the data records with purpose attributes/data fields
☒ Definition of database rights
☒ Separation of production and development environments

- **Pseudonymisation**
  The processing of personal data in such a way that the data can no longer be assigned to a specific data subject without additional information, provided that such additional information is kept separately and is subject to appropriate technical and organisational measures;

☒ Pseudonymisation of customer data (customer numbers)
☒ Pseudonymization in database applications (special tables for personal data and information)
☒ Data Protection Policy

2. Integrity

- Transmission control
  No unauthorized reading, copying, modification or removal during electronic transmission or transport, e.g.: Encryption, Virtual Private Networks (VPN), electronic signature;

☒ Installation of dedicated transmission paths or VPN tunnels
☒ Email encryption
☒ Documentation of the recipients of data and the time periods of the planned transfer or agreed deletion periods

- **Input control**
  Determining whether and by whom personal data have been entered, changes or removed in data processing systems, e.g.: Logging, document management;

☒

☒ Allocation of rights to enter, change and delete data based on an authorization concept

☒ Manual or automated control of the logs (according to strict internal specifications)

3. Availability and Resilience

- Availability control
  Protection against accidental or unintentionally destruction or loss, e.g.: Backup strategy (online/offline; on-site/off-site), uninterruptible power supply (UPS), malware protection, firewall, reporting procedures, incident response and emergency plans;
- Recoverability;

Uninterruptible power supply (UPS)

☒ Air conditioning in data centers

☒ Devices for monitoring temperature and humidity in data centers

☒ Fire and smoke detection systems

☒ Fire extinguishers in data centers

☒ Alarm message in case of unauthorized access to data center and similar areas

☒ Backup & recovery concept

☒ Tested data recovery processes

☒ Availability of an emergency plan

☒ Storage of data backup at a secure, external, outsourced location

☒ In flooded areas: data center above the waterline

4. Regular review, assessment, and evaluation procedures

☒ Review by Internal IT at the following intervals Annually

☒ Review by external consultants at the following intervals Annually

☒ Audit by certification authorities at the following intervals Annually

☒ Incident Response Management System in place

5. Privacy by design and by default;

☒ When purchasing devices and software, Privacy by Design / Privacy by Default is considered as a selection criterion

☒ During setup, the administrator activates specifically settings or options to implement Privacy by design / Privacy by default

☒ Data minimization is activated (only data necessary for the defined purpose are collected and stored..)

6. Processing on behalf of the Controller

No processors will be commissioned without privacy instructions from the controller

☒ Commission is processed via formalized evaluation process

☒ Selection of the processor / sub-processor according to data protection and data security criteria

☒ Preliminary examination of the data protection requirements at the order processor's premises

☒ Regular audits of the subcontractor / subcontractor

☒ The processor guarantees that the employees involved in processing the controller’s data and other persons working for the processor are prohibited from processing the data outside the scope of the controller’s instructions

☒

☒ The Processor warrants that the persons authorised to process the personal data have been bound to confidentiality or are subject to an appropriate statutory duty of confidentiality. The obligation to maintain confidentiality and secrecy shall continue to apply even after termination of the contract

7. Personnel Security and Training

☒ Click maintains personnel policies including having appropriate use guidelines, written confidentiality agreements

☒ Background checks are performed in accordance with Applicable Data Protection Laws

☒ Annual trainings on Information Security, Security Awareness, and Data Privacy are required of all employees and contractors

8. **Incident Response Management**

☒ Use of spam filter and regular updating

☒ Use of virus scanner and regular updating

Documented process for detecting and reporting security incidents / data breaches (also with regard to reporting obligation to supervisory authority)

☒ Formalized procedure for handling security incidents

☒ Documentation of security incidents and data breaches via ticket system

SCHEDULE 3 – SUBPROCESSORS

These subprocessors make up the infrastructure that supports **Click Marketing Automation, Sales Engagement, and CRM applications.**

Subprocessor	Geographic Location	Role	Data Transfer Mechanism
Microsoft Azure	US: North-Central AU: New South Wales EU: North Europe (IE) CA: Central Azure Data Center Locations	Cloud Service Provider for Click applications	Standard Contractual Clauses/Data Privacy Framework

Data center locations for Azure are chosen by the customer during the account registration process.

These subprocessors make up the infrastructure that supports the **email sending functionality** for **Click Marketing Automation**:

Subprocessor	Geographic Location	Role	Data Transfer Mechanism
MessageGears	US IE	Email Provider	Standard Contractual Clauses

Accounts hosted on the **EU data center** will use the Microsoft Azure EU/IE data center for Click hosting and the MessageGears EU/IE data center for email messaging.

Accounts hosted on the **US data center** will use the Microsoft Azure US data center for Click hosting and the MessageGears US data center for email messaging.

Accounts hosted on the **AU data center** will use the Microsoft Azure AU data center for Click hosting and the MessageGears US data center for email messaging.

Accounts hosted on the **CA data center** will use the Microsoft Azure CA for Click hosting data center and the MessageGears US data center with Secure PII for email messaging.

Minimal necessary data may be provided to a subprocessor outside an infrastructure location for purposes of providing Customer Support Services, as defined under Support and Services subprocessors.

These subprocessors make up the infrastructure that supports the **file management functionality** for **Click Marketing Automation**:

Subprocessor	Geographic Location	Role	Data Transfer Mechanism
UploadCare	US	File Management and Processing	Data Privacy Framework/Standard Contractual Clauses

These subprocessors make up the infrastructure that supports **Click Intelligent Dashboards**

Subprocessor	Geographic Location	Role	Data Transfer Mechanism
Amazon Web Services	North Europe (IE)	Cloud Service Provider for Click Intelligent Dashboards	Not Applicable – personal data is not transferred from the EU.
Google Cloud Platform	EU: Distributed	Cloud Service Provider for Click Intelligent Dashboards	Not Applicable – personal data is not transferred from the EU.

Embedded Functionality

These subprocessors provide additional functionality in the application

Subprocessor	Geographic Location	Role	Data Transfer Mechanism
Oktopost	US	Social Posting	Standard Contractual Clauses / Data Privacy Framework

Support and Services

These subprocessors are used to provide customer support for our Services

Subprocessor	Geographic Location	Role	Data Transfer Mechanism

Allbound	US	Customer Support Services	Standard Contractual Clauses
Microsoft 365	US	Customer Support Services	Standard Contractual Clauses / Data Privacy Framework
OneTrust	US	Customer Support Services	Standard Contractual Clauses / Data Privacy Framework
Pendo	US	Customer Support Services	Standard Contractual Clauses
Raia AI	US	Customer Support Services	Standard Contractual Clauses
TL;DV	US	Customer Support Services	Standard Contractual Clauses
Zendesk	US	Customer Support Services	Standard Contractual Clauses / Data Privacy Framework

Affiliates

The following affiliate companies are members of ClickDimensions, LLC and function as subprocessors

Subprocessor	Geographic Location	Role	Data Transfer Mechanism
ClickDimensions Ireland	IE	Customer Success and Support	N/A
ClickDimensions Spain	ES	Research & Development	N/A
ClickDimensions APAC Limited	NZ	Customer Success and Support	Adequacy