Unilink

UNILINK DATA PROCESSING AGREEMENT

This ***Data Processing Agreement*** (hereinafter referred to as: "***Data Processing Agreement***", or "***the Agreement***") entered into by and between ***Client*** (as defined under the Terms and Conditions) (hereinafter referred to as: "***Client***" or "***You***", "***Your***", "***Yours***") and ***the Company*** (as defined under the ***Unilink Terms and Conditions)*** (hereinafter referred to as "***the Company***", "***Us***" or "***We***") forms an integral part of, and is subject to, ***Unilink Terms and Conditions*** available at ***https://unilink.io/documents***

Client and ***the Company*** are hereinafter jointly referred to as the "***Parties***" and individually as the "***Party***". Capitalized terms not otherwise defined herein shall have the meaning given to them in ***Unilink Terms and Conditions***. In the event of any conflict between ***Unilink Agreement*** and ***Unilink Terms and Conditions***, the terms of ***the Agreement*** shall prevail.

The Agreement only applies to the extent where the EU Data Protection Law are applicable to ***the Processing*** of ***Personal Data*** under ***the Agreement***, including if (a) ***the Processing*** is carried out in the context of the activities of an establishment of either Party in the European Economic Area ("EEA"), and/or (b) ***the Personal Data*** relates to ***Data Subjects*** who are in the EEA and the ***Processing*** relates to the offering to them of goods or services or the monitoring of their behavior in the EEA.

1.DEFINITIONS

1. "***Controller***" shall mean the entity which determines the purposes and means of the ***Processing*** of ***Personal Data***.
2. "***Processor***" or "***Data Processor***" means the entity which ***Processes Personal Data*** on behalf of ***the Controller***.
3. "***Personal Data***" shall mean any information relating to an identified or identifiable person as defined in Article 4.1 of ***the GDPR*** *i.e.* any information relating to an identified or identifiable natural person ('***Data Subject***'); 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 the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

4. "***Data Subject***" shall mean the individual, determined hereinabove to whom ***Personal Data*** relates, including ***End Users***.
5. "***End User***" shall mean the end user of an internet connected device, such as a visitor to a web page, a user of a mobile app, or a user of an IoT device, or a visitor on advertisement or campaign webpage.
6. "***the GDPR***" shall mean Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (also known as "***General Data Protection Regulation***").
7. "***Processing***" shall mean any operation or set of operations which is performed on ***Personal Data*** or on sets of ***Personal Data***, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction ("***Process***", "***Processes***" and "***Processed***" shall have the same meaning).
8. "***Sub-Processor***" shall mean any ***Processor*** engaged by the ***Processor***.
9. "***Services***" shall mean services provided by ***the Company*** via Unilink software in accordance with ***Unilink Terms and Conditions***.

2. PROCESSING OF PERSONAL DATA

2.1. Under ***the Agreement*** and with respect to ***Personal Data***, ***Client*** is ***Controller*** or ***Processor*** and the ***Company*** is engaged by ***Client*** as ***Processor*** or another ***Processor*** (***Sub-Processor***) in respect to ***Personal Data***, as applicable. The terms of ***the Agreement*** shall apply to either of the relations between ***the Parties*** regarding ***the Processing*** of ***Personal Data*** mentioned herein.

2.2. Within the scope of ***the Agreement***, ***Client*** hereby engages ***Processor*** to collect, process and/or use ***Personal Data*** on behalf of ***Client***.

2.3. ***Processor*** will only ***Process Personal Data*** on ***Your*** behalf and in accordance with ***Your*** documented instructions. The instructions from ***the Client*** to ***Process Personal Data*** are the following: (i) ***Processing*** shall be carried out in accordance with ***the Agreement***, ***the Terms and Conditions*** and pursuant to the features and limitations of the applicable ***Services*** which ***Processor*** provides to ***Client***; and (ii) ***Processing*** shall be carried out in compliance with other reasonable instructions provided by ***the Client***, where such

instructions are consistent with ***Unilink Terms and Conditions***. ***The Company*** shall be under no obligation to comply with the documented instructions that ***the Company*** deems as violating applicable laws. ***Processing*** outside the scope of the Agreement (if any) shall require: *(i)* prior written agreement between ***Client*** and ***the Company***, and *(ii)* ***Client's*** additional instructions for ***Processing***.

2.4. ***The Company*** employs ***the Personal Data*** solely to provide ***the Services*** in accordance with ***Unilink Terms and Conditions***, i.e. in order to perform tracking services / serve ***End Users*** with interest–based advertising, as well as to measure the effectiveness of advertising campaigns and provide ***You*** with advertising reports. In that context, ***the Company*** – on ***Your*** demand – may also combine ***Personal Data*** from different sources in order to improve ***Services*** and integrate ***Services*** with external platforms, all of which will be conducted on ***Your*** behalf. ***The Company*** also ***Processes Personal Data*** on ***Your*** behalf and to serve ***Your*** interests for the purposes of fraud prevention, bot detection, rating, analytics, viewability, ad security services. ***The Company*** may also ***Process*** data based on the extracts of ***Personal Data*** in aggregated and non-identifiable forms, including for the purposes of testing, development, control and operation of ***the Services***.

2.5. The may ***Process*** the following ***Data*** on ***Your*** behalf: IP addresses, language information, session-based browsing behavior, header information, ***End User's*** device-related data (such as the type or model of the device), operating system, wireless carrier providing communication services to such device, geographical location (geo-location) of the device, cookies, advertising identifiers of the device, as well as other information we may receive from ***You*** or from third parties engaged by ***the Company*** on ***Your*** behalf, such as non-precise device location based on the IP address, device specifications and user's interest's information. ***Client*** also authorises ***the Company*** to store and use cookies or pixel tags on ***End User's*** device on behalf of ***the Client*** in order to perform ***Services***. Additional information regarding the types of ***End User's Data*** that may be collected or used by ***the Client*** through ***Services*** are specified in ***End User Privacy Policy***.

2.6. Without derogating from any of the obligations of ***the Client*** hereunder, ***the Client*** shall not provide ***the Company*** with any ***Data***: *a)* which by itself identifies an individual, such as name, address, phone number, email address; and b) regarding children, or any special categories of ***Personal Data***, as defined under ***Article 9 of the GDPR***, except as may otherwise be expressly agreed in writing between ***the Parties*** and in accordance with the applicable law. This type of ***Data*** is not necessary to use ***the Company's Services***.

2.7. ***Client*** is responsible for ensuring their own compliance with various laws and regulations, including ***the GDPR***. To the extent required under the applicable law, ***Client*** shall provide an appropriate notice to ***Data Subjects*** about ***the Processing*** of their ***Personal Data*** in connection with the use of ***Services*** under ***the Agreement*** and under ***Unilink End User Privacy Policy***, and ***You*** shall receive and document ***the Data Subjects***' consent thereof to the extent required under the applicable law.

2.8. To the extent required under the applicable law, ***Client*** has to also use commercially reasonable efforts to ensure that ***the End User*** is provided with clear and comprehensive information about ***Cookies*** or other information on ***the End User's*** device in connection with the use of ***Services*** by ***the Client*** and, if applicable, consents to their storing and accessing. To the extent required under the applicable law, ***Client*** shall inform ***the End User*** about third party ***Cookies*** (or other tracking technologies) which may be placed on ***Client's*** site(s), specifying the purpose of these ***Cookies*** (e.g., targeted advertising) and the type of ***Data*** collected on ***the Client's*** site(s). ***Client*** shall also inform ***End Users*** of options to deactivate ***Company's Cookies*** by including in its privacy policy a link to the ***Unilink End User Privacy Policy*** and when legally compulsory, appropriate notice, consent and choice mechanisms that comply with relevant laws and regulations, including ***the GDPR***.

2.9. ***Client*** acknowledges and agrees that ***the Client*** shall retain sole responsibility for the lawfulness of ***the Processing*** and shall warrant to the company that ***the Client*** is legally allowed to engage ***the Company*** to ***Process Personal Data*** on ***Client's*** behalf, has provided all necessary notices and obtained all required consents from the ***Data Subjects*** (if apply) for the purposes of the ***Processing*** described in ***the Agreement***.

3. RIGHTS OF DATA SUBJECTS

3.1. ***The Company*** shall notify ***Client*** via email, if it receives a request from a ***Data Subject*** that concerns access to, correction, amendment, deletion of or objection to ***the Processing*** of that ***Data Subject's Personal Data***. ***The Company*** shall not respond to any such ***Data Subject*** request without ***Client's*** prior written consent, except in order to confirm that the request relates to ***the Client***.

3.2. To the extent that ***Client*** responds to any such ***Data Subject*** request, ***the Company*** shall provide ***Client***, to the extent required by law, with commercially reasonable cooperation and assistance in relation to handling of a ***Data Subject's*** request, to the extent legally permitted.

3.3. ***The Company*** reserves the right to charge additional fees in relation to the cooperation with ***the Client*** in regard to ***the Agreement***.

4. COMPANY'S PERSONNEL

4.1. ***The Company*** shall ensure that its personnel engaged in ***the Processing*** of ***Personal Data*** is informed of the confidential nature of ***the Personal Data***, and is subject to obligations of confidentiality. Such obligations shall survive the termination of that individual's engagement with ***the Company***.

4.2. ***The Company*** shall ensure that access to ***Personal Data*** is limited only to those members of personnel who require that access in order to fulfil ***the Company's*** obligations under ***Unilink Terms and Conditions***.

5. SECURITY

5.1. Pursuant to Article 28(3c) of ***the GDPR, the Company*** shall take the measures required by the Article 32 of ***the GDPR***.

5.2. ***The Company*** shall provide sufficient guarantees of implementation of the appropriate technical and organizational measures in a manner that the processing will meet the requirements of ***the GDPR*** and ensure the protection of the rights of the ***Data Subject***.

5.3. ***The Company*** imposes appropriate contractual obligations upon its personnel that engages in ***the Processing*** of ***Personal Data***, including relevant obligations regarding confidentiality, ***Data*** protection and ***Data*** security. ***The Company*** ensures that its applicable personnel has been properly informed of the confidential nature of ***the Personal Data***.

6. AUDIT RIGHT

6.1. To the extent that the applicable law requires ***the Client*** to be in a position to monitor the adequate ***Processing*** of ***Personal Data***, ***You*** as ***the Client*** has the right to request an audit from ***the Company*** to the extent necessary to review whether we as the Company and ***Our Sub-Processors*** are compliant with the following regulations: (i) any provisions of the Law, (ii) the terms of this ***Agreement***, and (iii) ***Client's*** instructions.

6.2. ***The Company may*** provide ***Client*** with a copy of its most recent third-party certifications issued by an independent, third-party auditor, as applicable, or any summaries thereof in order to fulfil ***Client's*** audit rights - as applicable. If an audit is required by law and

where its requirements cannot be fulfilled by the provision of such certification, ***Client*** may conduct, either by yourself or through a third party independent contractor selected by ***Client*** and approved by ***the Company***, at ***Client's*** expense, an on-site audit of ***the Company***. Such audit may be conducted subject to the following terms and conditions: (*i*) the audit will be pre-scheduled in writing with ***the Company*** at least 60 days in advance and will be performed once a year at most; (*ii*) if applicable, all of ***Client's*** personnel performing the audit, whether employed or contracted by ***the Client***, will execute a ***Company's*** standard non-disclosure agreement prior to the initiation of the audit, and a third party auditor will in addition execute a non-competition undertaking; (*iii*) ***Client*** will undertake all necessary measures to ensure and verify that the auditors do not access, disclose or compromise the confidentiality and security of ***Personal Data*** other than ***Client's Personal Data*** on ***Company's*** information and network systems; (*iv*) ***Client*** will take all necessary measures to prevent any damage or interference with ***Company*** or its service providers' information and network systems; (*v*) ***Client*** will bear all costs and assume responsibility and liability for the audit and for any failures or damage caused as a result thereof; and (*vi*) any audit activities on ***Company's*** third-party service providers' information systems will be pre-scheduled and agreed on with the applicable providers; (*vii*) ***Client*** will keep the audit results in strict confidentiality, use them solely for the specific purposes of the audit under Section 6 hereof and ***the GDPR*** will not use the results for any other purpose, or share them with any third party, without the ***Company's*** prior explicit confirmation in writing; (*viii*) If ***Client*** are required to disclose the audit results to a competent authority, ***Client*** will provide ***the Company*** with a prior written notice, explaining the details and necessity of the disclosure, as well as provide all further necessary assistance to prevent such disclosure.

7. SECURITY BREACH MANAGEMENT AND NOTIFICATION

If ***the Company*** becomes aware of any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to any ***Personal Data*** transmitted, stored, or otherwise ***Processed*** on equipment being employed by ***the Company*** or in ***the Company's*** facilities (hereinafter referred to as: "***Security Breach***"), ***the Company*** shall with reasonable despatch: (i) notify ***the Client*** of ***the Security Breach***; (ii) in depth investigate ***the Security Breach*** and provide ***Client*** with all relevant information about ***the Security Breach***; and (iii) take all commercially reasonable steps to mitigate the effects and minimize any damage resulting from ***the Security Breach***.

Unilink

8. SUBPROCESSING AND TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES

8.1. ***Client*** authorises ***the Company*** to appoint ***Sub-Processors*** in order to provide ***the Services***.

8.2. ***The Company*** may continue to use ***the Sub-Processors*** already engaged by ***the Company*** according to ***the Agreement***.

8.3. It is acknowledged and agreed by ***the Client*** that as of the date of ***the Agreement***, ***the Company*** uses the following ***Sub-Processors*** for the purpose of providing its ***Services***:

Amazon Web Services Inc. Cloud hosting services Privacy Shield Framework Principles issued by the U.S. Department of Commerce, located at

https://privacyshield.gov/

Google Analytics
https://policies.google.com/privacy

Facebook Pixel
https://www.facebook.com/business/help/651294705016616

Google AdWords
https://www.google.com/policies/technologies/ads/

LinkedIn Insight Tag
https://www.linkedin.com/legal/privacy-policy

Twitter Pixel
https://twitter.com/en/privacy

Universal Event Tracking by Bing Ads
https://privacy.microsoft.com/en-US/privacystatement

Livechat Inc.
https://www.livechatinc.com/general-data-protection-regulation/

Zendesk
https://help.zendesk.com/hc/en-us/articles/229138227-Privacy-and-Data-Protection-How-Zendesk-Protects-Personal-Data-

8.4. ***Client*** authorises ***the Company*** to appoint new ***Sub-Processors*** and give notice of the appointment of any new ***Sub-Processor*** via email or announcement on its website.

8.5. ***The Company*** may integrate ***the Client's*** services with external service providers' platforms for the purpose of providing its ***Services***, on ***Client's*** behalf and for the purposes of serving the ***Client's*** interests, where such external service providers may be ***Sub-Processors***, which ***Client*** hereby agrees to.

8.6. Notwithstanding the provisions above, ***Client*** hereby authorises ***the Company*** to subcontract ***the Processing*** to ***the Sub-Processors*** based outside of the European Economic Area (EEA) to the extent necessary to duly perform ***the Service(s)***, under the condition that ***the Sub-Processors*** will provide sufficient guarantees in relation to the required level of data protection, e.g. through a Privacy Shield certification according to the EU Commission Decision 2016/1250, or a subcontracting agreement based on the standard contractual clauses launched by virtue of the EU Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC or ***the GDPR*** (hereinafter referred to as: "***Model Contract Clauses***"), or based on other applicable transborder data transfer mechanisms.

9. TERM AND RETENTION PERIOD

9.1. The Agreement shall become effective as of May 25, 2018.

9.2. ***Client*** authorises ***the Company*** to retain ***Personal Data*** for a period of 3 years from the date of its collection on ***Client's*** behalf and for the purpose of serving its interests, including for fraud prevention, ad security services, reporting services, complaints or chargebacks handling. This ***Data*** may be deleted from ***the Company's*** servers after this retention period and/or after the termination of ***the Agreement*** or earlier, at your written request.

10. INDEMNIFICATION AND LIMITATION OF LIABILITY

10.1. ***Client*** shall indemnify and hold ***the Company***, its officers, directors, employees, contractors, and agents harmless from and against all claims, liabilities, administrative fines, suits, judgments, actions, investigations, settlements, penalties, fines, damages and losses, demands, costs, expenses, and fees including reasonable attorneys' fees and expenses, arising out of or in connection with any claims, demands, investigations, proceedings, or actions brought by data subjects, legal entities (e.g., corporations and organizations etc.), or supervisory authorities under the data protection laws that apply to ***the Company*** in respect of ***Processing*** of ***Personal Data*** on behalf of ***Client*** through ***Services***.

10.2. The liability of each party under ***the Agreement*** shall be subject to the exclusions and limitations of liability set out in ***Unilink Terms and Conditions***.

11. GOVERNING LAW

11.1. ***The Agreement*** shall be governed by, and is construed in accordance with, the laws of England and Wales, without giving any effect to any choice of law and provisions thereof that would cause the application of the laws of any other jurisdiction.