DATA PROCESSING AGREEMENT

This Data Processing Agreement ("DPA") is hereby entered by and between Prime Time Advertising LP and the undersigned counterparty on behalf of itself and its Affiliates (collectively "Company"), each a "party" and collectively, the "parties". This DPA sets forth the parties' responsibilities and obligations regarding the Processing of Personal Data, including without limitations internet protocol ("IP") address, IDs (as defined below) and similar online identifiers, during the course of the parties' engagement under the Insertion Order previously signed between the parties ("IO").

This DPA forms an integral part of the IO and amends any previously terms relating to the Processing of Personal Data. This DPA shall be effective as of parties' signature date if such date is before May 25, 2018; or as of May 25, 2018 Company's signature date is made following such date ("Effective Date").

Capitalized terms not defined herein shall have the respective meanings given to them in the IO.

1) Definitions

1.1 "Affiliates" means any entity which is controlled by, controls or is in common control with one of the parties.

1.2 "Data" means any and all Data Subject's data collected through the course of the Agreement or shared between the parties that may include, inter alia, demographic data, device information, Ad IDs, cookies, browsing URLs, apps installed and/or accessed, events, and geo localization data. The Data includes, without limitation, data deemed as Personal Data.

1.3 "Data Protection Law" means any and all applicable privacy and data protection laws and regulations (including, where applicable, EU Data Protection Law) as may be amended or superseded from time to time.

1.4 "Controller", "Processor", "Data Subject", "Personal Data", "Processing" (and "Process"), "Personal Data Breach", "Special Categories of Personal Data" and "Supervisory Authority" shall have the meanings given in EU Data Protection Law.

1.5 "EU Data Protection Law" means the (i) EU General Data Protection Regulation (Regulation 2016/679) ("GDPR"); (ii) the EU e-Privacy Directive (Directive 2002/58/EC), as amended (e-Privacy Law); (iii) any national data protection laws made under, pursuant to, replacing or succeeding (i) and (ii); (iv) any legislation replacing or updating any of the foregoing (v) any judicial or administrative interpretation of any of the above, including any binding guidance, guidelines, codes of practice, approved codes of conduct or approved certification mechanisms issued by any relevant Supervisory Authority.

1.6 "ID" means (i) a unique identifier stored on an end-user's device, (ii) a unique identifier generated on the basis of device information, or (iii) a resettable advertising ID associated with a mobile device or an application.

1.7 "Security Incident" means any security breach relating any Personal Data elements leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data within, Personal Data transmitted, stored or otherwise processed; including without limitation the meaning assigned to it under paragraph 12 of Article 4 of the GDPR. For the avoidance of doubt, any Personal Data Breach of the other Party's Personal Data will comprise a Security Breach.

2) Applicability

This DPA applies solely to the extent that Data Protection Law applies to the Processing of Personal Data under the Agreement, including if (i) the Processing is in the context of the activities of an establishment of either party in the European Economic Area ("EEA") or (ii) 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 by or on behalf of a party. Notwithstanding the above, this DPA does not apply to aggregated reporting or statistics information a party may collect from Data Subject or provide to the other party.

3) Parties' Roles

The parties agree and acknowledge that under the performance of their obligations set forth in the IO, and with respect to the Processing of Personal Data, Prime Time Advertising LP is acting as a Data Processor and the Company is acting as Controller. Each party shall be individually and separately responsible for complying with the obligations that apply to it under applicable Data Protection Law.

4) Processing of Personal Data and Compliance with Data Protection Law

4.1 In performing its obligations under the Agreement, the parties may provide Personal Data to the other party. Each party shall collect, process and share Personal Data in compliance with applicable Data Protection Law, industry standards and its obligations herein.

4.2 Without derogating from the general or specific terms herein, the Company hereby warrants and represents that as of May 25, 2018 it will be compliant with EU Data Protection Law, and it shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Company obtained Personal Data.

4.3 During the Term of the IO, Prime Time Advertising LP shall only Process Personal Data on behalf of and in accordance with and shall treat Personal Data as Confidential Information. Company instructs Prime Time Advertising LP to Process Personal following purposes: (i) Processing in accordance with the IO in order to provide the Prime Time Advertising LP Services; (ii) in order to comply with additional instructions provided by the Company and agreed in written between the parties, which shall ensure that its instructions for the Processing of Personal Data shall comply with the Data Protection Law.

4.4 The Company sets forth the details of the Processing of the Personal Data under the IO, as required by Article 28(3) of the GDPR in Schedule 1, attached hereto.

4.5 Prime Time Advertising LP may Process Personal Data other than as instructed by the Company if it is mandatory under law. Prime Time Advertising LP shall make reasonable efforts to inform the Company of such requirement unless prohibited applicable law.

4.6 Each party shall identify and provide contact details for its contact point within its organization authorized to respond to enquiries concerning Processing of the Personal Data or its Data Protection Officer ("DPO"), as applicable. In the event of a change of the above contact person or DPO's identity, each party shall provide updated contact details.

5) Privacy Policy, Consent Requirements & Rights of the Data Subject

5.1 As between the parties, the Company undertakes accepts and agrees that the Data Subject do not have a direct relationship with Prime Time Advertising LP and that Prime Time Advertising LP relies on legitimate interest or consent (if Protection Law) as its legal basis to Process Personal Data. In the event consent is needed under Data Protection Law, the Company shall ensure that it obtains a proper act of consent from Data Subjects and all necessary and appropriate notices in accordance with applicable Data Protection Law and other relevant privacy requirements in

order to Process Personal Data and enable lawful transfer of the Personal Data to S&W for the duration and purposes set forth in the IO and herein, as well as in order to enable the data collection in order to provide the S&W Services under the IO, as detailed in S&W's privacy policy available at: http://www.snw.media/wp-content/uploads/2018/01/Privacy-Policy-1.pdf ("Privacy Policy"). In the event Data Subject consent is required under Data Protection Law, Company shall maintain a record of all consents obtained from Data Subject, including the time and data on which consent was obtained, the information presented to Data Subject in connection with their giving consent, and details of the mechanism used to obtain consent, as well as a record of the same information in relation to all withdrawals of consent by Data Subject. Company shall make these records available to S&W promptly upon request.

5.2 Without derogating from the Company's obligations hereunder, the Company may only provide S&W, the Personal Data types and parameters which are explicitly permitted under S&W's Privacy Policy. The Company shall be solely liable for any Data which is provided or otherwise made available to S&W or anyone on its behalf in excess of the Personal Data permitted therein.

5.3 Unless otherwise agreed to in writing by the parties, the parties shall not share Personal Data that allows Data Subjects to be directly identified (e.g., name or email) or any Personal Data that contains Personal Data relating to children under 16 years old (or lower age to the extent required by applicable law). In addition, Special Categories of Personal Data shall not be Processed or shared in connection with the performance of each party's obligations under the IO.

5.4 The Company shall maintain a publicly-accessible privacy policy on its mobile applications, websites or any other applicable digital assets that is available via a prominent link that satisfies transparency disclosure requirements of Data Protection Law.

5.5 It is agreed that where either party receives a request from a Data Subject or an applicable authority in respect of Personal Data Controlled or Processed by the other party, where relevant, the party receiving such request will direct the Data Subject or the authority to the other party, as applicable, in order to enable the other party to respond directly to the Data Subject's request. Each party shall reasonably cooperate and assist the other party in handling of a Data Subject's or an authority's request, to the extent permitted under Data Protection Law.

6) Sub-Processor

6.1 Company acknowledges that in the provision of the S&W's Services, S&W may transfer Personal Data to and otherwise interact with third party data processors ("Sub-Processor"). Company authorizes S&W to engage and appoint such Sub-Processors to Process Personal Data, as well as permits each Sub-Processor to appoint a Sub-Processor on its behalf.

6.2 S&W may continue its engagement with its current Sub-Processors as of the date of this DPA, which engagement is subject to the respective Sub-Processors terms and applicable guidelines.

6.3 In the event S&W appoints a new Sub-Processor, it shall provide a notice of the appointment of any new Sub-Processor (for instance as part of a Privacy Policy amendment or by any other notification, as S&W deems applicable in its sole discretion), whether by general or specific reference to such Sub-Processor (e.g., by name or type of service), including relevant details of the Processing to be undertaken by the new Sub Processor ("Sub-Processor Notice").

6.4 The Company may object the appointment of the new Sub-Processor, as follows:

6.4.1 The Company may provide S&W, within seven (7) days of Sub-Processor Notice, with a written notification stating its objection, based on reasonable grounds, to the appointment of the New Sub-Processor.

6.4.2 S&W may not appoint for the processing of Company's Personal Data the proposed Sub-Processor until reasonable steps have been taken to address the objections raised by Company. S&W shall provide the Company with a written notification detailing the steps taken in this regard.

6.4.3 Within three (3) days of receipt of S&W's notice regarding the steps taken as detailed in Section 6.4.2 above, the Company may notify S&W it does not find such steps taken by S&W sufficient to settle its objections. In the event the Company have not provided such notification, it will constitute Company's approval of the Sub Processor. In the event the Company further object, each party may terminate the IO upon a written notification effective immediately, without liability.

6.5 S&W will enter into separate contractual arrangements with such Sub-Processors binding them to comply with obligations in accordance with Data Protection Law.

7) Return and Deletion of Personal Data

7.1 Subject to Section 7.2, S&W shall promptly and in any event within up to sixty (60) days of the date of cessation the IO, delete or pseudonymize all copies of those Personal Data obtained through the Company, except such copies as authorized or required to be retained in accordance with applicable law and/or regulation.

7.2 S&W may retain the Personal Data to the extent authorized or required by applicable laws, provided that S&W shall ensure the confidentiality of all such Personal Data and shall ensure that it is only processed for legal purpose(s).

8) Technical and Organizational Measures & Security Incident

8.1 Each party shall implement appropriate technical and organizational measures to protect the Personal Data and its security, confidentiality and integrity and the Data Subject's rights, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing the Personal Data, as well as the risk of varying likelihood and severity for the consumer's rights, in order to ensure a level of security appropriate to that risk, including measures such as access control, auditing, encrypted transmission of data, encrypted storage and physical protections in-line with industry best practices, in accordance Data Protection Laws.

8.2 Description of the technical and organizational measures implemented by S&W, are available at: http://www.snw.media/wp-content/uploads/2018/01/Privacy-Policy-1.pdf ("Security Information Page"). S&W may update or modify the Security Information Page from time to time provided that such updates and modifications will not result in the degradation of the overall security of the Personal Data.

8.3 S&W shall take reasonable steps to ensure that its personal access to the Personal Data is limited on a need to know or access basis, and that its personnel receiving such access are subject to confidentiality undertakings or professional or statutory obligations of confidentiality in connection with their access or use of the Personal Data.

8.4 The Company hereby confirms that the Security Information Page detailed above provide an appropriate level of protection for the Company's Personal Data Processed through the S&W Services, taking into consideration the nature of Personal Data and the risks associated with the Processing of the Personal Data.

8.5 In the event that S&W or Company suffer a confirmed Security Incident, each party shall notify the other party, by means of any applicable communication, without undue delay. The parties shall cooperate in good faith to agree and action such measures as may be necessary to mitigate or remedy the effects of the Security Incident.

8.6 A notification of a Security Incident by S&W shall not constitute an acknowledgement by S&W of any liability with respect to applicable Personal Data related to the Security Incident.

9) Audit Rights

9.1 Subject to the terms of this Section , S&W shall make available to a reputable auditor nominated by the Company in coordination with S&W, upon prior written request and solely once per year, such information necessary to reasonably demonstrate compliance with this DPA, and shall allow for audits, including inspections, by such reputable auditor solely in relation to the Processing of the Personal Data provided by the Company, and subject to a written confidentiality obligations signed by the auditor ("Audit"). In any event, the Audit shall be subject to the terms of this DPA, and to S&W's obligations to third parties, including with respect to confidentiality. S&W may object in writing to an auditor appointed by the Company in the event S&W reasonably believes, the auditor is not suitably qualified or independent, a competitor of S&W or otherwise manifestly unsuitable ("Objection Notice"). In the event of Objection Notice, the Company will appoint a different auditor or conduct the Audit itself.

9.2 Company shall bear all expenses related to the Audit and shall reimburse S&W for all such expenses occurred to it due to the Audit, and shall make (and ensure that each of its mandated auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimize) any damage, injury or disruption to S&W's premises, equipment, personnel and business while its personnel are on those premises in the course of such Audit.

9.3 The Company shall provide S&W with a reasonable prior written request for any Audit or inspection to be conducted. The parties shall mutually agree upon the scope, timing and duration of the Audit or inspection in addition to the reimbursement rate for which Company shall be responsible.

9.4 It is hereby agreed that the Audit will be conducted as follows: (i) upon Company's written request, S&W will provide the Company or its appointed auditor with the most recent certifications and/or summary audit report(s), which S&W has procured to regularly test, assess and evaluate the effectiveness of its security measures; (ii) S&W will reasonably cooperate with the Company by providing available additional information concerning the security measures; (iii) in the event further information is needed by the Company in order to comply with a competent Supervisory Authority's request, the Company will inform S&W in writing to enable it to provide such information or to grant needed access, at S&W's sole discretion; (iv) solely to the extent the above does not enable the Company to satisfy an audit obligation mandated by applicable law or legally mandated entities, the Company or its appointed auditor may conduct an onsite visit of the facilities used to provide the S&W Service and under S&W's control. Such visit will occur with at least 30 days' prior written notice, during normal business hours and only in a manner that causes minimal disruption to S&W's business, and in accordance with any audit procedures reasonably required by S&W in order to protect its data and business.

9.5 The Company shall promptly notify S&W with information regarding any non-compliance discovered during the course of an Audit.

10) Data Transfer

Where EU Data Protection Law applies, neither party shall transfer to a territory outside of the EEA unless it has taken such measures as are necessary to ensure the transfer is in compliance with EU Data Protection Law. Such measures may include (without limitation) transferring the Personal Data to a recipient in a country that the European Commission has decided provides adequate protection for Personal Data.

11) Liability

11.1 Each party shall take out and maintain insurance policies to the value sufficient to meet their respective liabilities under or in connection with this DPA and the Agreement. Upon a party's request, the other party will provide evidence that such insurance is in place.

11.2 The total combined liability of either party towards the other party and its Affiliates under or in connection with the DPA will be limited to any liability cap set forth in the IO.

12) General.

12.1 The parties to this DPA hereby submit to the choice of jurisdiction stipulated in the IO with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity.

12.2 This DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the IO.

12.3 In the event of any conflict or inconsistency between this DPA and S&W's Privacy Policy, S&W's Privacy Policy shall prevail provided only that the procedure prevailing through the Privacy Policy shall not constitute as a breach or infringement of any Data Protection Laws. In the event of inconsistencies between the provisions of this DPA and the IO, terms of this DPA shall prevail.

12.4 This DPA is not intended to, and does not in any way limit or derogate from Company's own obligations and liabilities towards S&W under the IO, and/or pursuant to the EU Data Protection Laws.

12.5 Nothing in this DPA shall confer any benefits or rights on any person or entity other than the parties to this DPA.

Schedule 1

Details of Processing of Controller Personal Data

This Schedule 1 includes certain details of the Processing Personal Data as required by Article 28(3) GDPR.

Subject matter and duration of the Processing of Personal Data

As set out in the IO and S&W's Privacy Policy incorporated therein.

The nature and purpose of the Processing of Personal Data

To provide the S&W Services, as detailed in the IO, including without limitation to display advertising to Data Subjects and optimizing performance.

The types of Personal Data to be Processed

ID's, as shall be amended from time to time according to S&W's Privacy Policy.

The categories of Data Subject to whom the Personal Data relates

Company's end users to which Data Protection Law applies and its Personal Data is provided to S&W in order to provide the S&W's Services. The obligations and rights of the Company are set out in the IO and this DPA.

The obligations and rights of the Company and its Affiliates

As set out in the IO and this DPA.