Amplify Data Sharing Agreement – **EXTRACT**

Amplify Data Sharing Agreement

This Data Sharing Agreement ("**DSA**") is entered into by the Outbrain entity ("**Outbrain**") and the individual or company (the "**Customer**") identified in the Insertion Order (governed by the applicable Amplify Terms and Conditions) between the parties from time to time (together, the "**Terms**") and/or using the Dashboard and governs the processing of Personal Data pursuant to the provision of the Service by Outbrain. This DSA shall apply to any and all agreements between the parties and their Affiliates from time to time.

This DSA is incorporated into the Terms (as amended from time to time) and constitutes a legally binding agreement between the parties. Collectively, the Controller SCCs (as applicable), the DSA and the Terms (or information entered through the Dashboard) are referred to as the "**Agreement**". In the event of any conflict or inconsistency between any of the terms of the Agreement the following order of precedence shall prevail: (i) the Controller SCCs (as applicable); (ii) this DSA; and (iii) the Terms.

Any capitalized terms not defined in this DSA shall have the respective meanings given to them in the Terms.

4. ROLE OF PARTIES.

4.1. Each party shall comply with all relevant provisions of Data Protection Laws as it applies to matters under the Agreement and ensure that they process Personal Data fairly and lawfully in accordance with Data Protection Laws as applicable in the provision and receipt of the Service.

4.2. Insofar as the CCPA is applicable to the Service, Outbrain and Customer will be considered independent Businesses under the CCPA for the collection, processing and selling of any Personal Information, and Outbrain shall not be considered a Service Provider on anyone's behalf.

4.3.Insofar as EU Data Protection Laws are applicable to the Service, the parties shall be deemed Joint Controllers under Article 26 GDPR solely with regards to the implementation of Outbrain Pixel by Customer, and the parties shall be deemed independent Controllers for any other processing activity. In particular, the Customer shall strictly remain independent controller for any Third Party Targeting.

4.4. Each party shall remain solely and exclusively responsible for determining the means and purposes of processing for its respective processing activities.

5. CUSTOMER'S OBLIGATIONS.

5.1.Customer represents and warrants that its use of Pixels or Third Party Targeting shall, at all times, be compliant with Data Protection Laws and satisfy the requirements for an appropriate legal basis for processing.

5.2.Customer shall not, at any time, use Third Party Targeting: (i) for discriminatory purposes; (ii) to target minors under the age of sixteen(16); (iii) based on Special Categories of Personal Data; (iv) based on Personal Data relating to alleged or confirmed criminal convictions or offenses; or (v) otherwise in violation of any applicable law in any country where the campaign is performed.

5.3.Customer shall disclose to End Users, via an appropriate privacy notice, that it uses Third Party Targeting and/or Pixels, including an explanation that third parties, including Outbrain, may use cookies or similar technologies to collect or receive Personal Data from Customer's website(s) or application(s), and may use that Personal Data for the purposes detailed in Section 2. Such privacy notice shall offer to End Users, as applicable, a consent or opt out choice mechanism regarding the collection and sharing of their Personal Data with third parties, including Outbrain (including, under the CCPA, a "Do Not Sell My Personal Information" option) in compliance with applicable Data Protection Laws.

5.4. When implementing Outbrain Pixel on their website(s) or application(s), Customer shall, either:

(i) Insofar as EU Data Protection Laws are applicable to the Service, use a consent management platform using the IAB Transparency & Consent Framework v2.0 (the most recent version or successor thereto) and pass Outbrain valid "consent"/"no consent" strings; or

(ii) Insofar as the CCPA is applicable to the Service, collect "Do Not Sell My Personal Information" choices via a consent management platform using the IAB CCPA Framework (the most recent version or successor thereto) and pass Outbrain valid "yes"/"no" strings; or

(iii) Where the Customer does not use any of the above consent management platforms, if an End User opted out or withdrew their consent to personalized advertising via Customer's website(s) or a mechanism such as a setting within a Customer's application(s), Customer shall be fully responsible for not loading the Outbrain Pixel.

5.5. Customer shall be fully responsible to ensure that no more Personal Data than necessary is shared with Outbrain via the Outbrain Pixel.

6. OUTBRAIN'S OBLIGATIONS.

6.1. Outbrain shall disclose, via an appropriate privacy notice, all information relating to processing activities where the Personal Data is collected directly from the End User or where such Personal Data is collected via third parties, as required under Data Protection Laws. This information is available on Outbrain's Privacy Policy.

6.2. Outbrain shall at all times satisfy the requirements for an appropriate legal basis for the processing of Personal Data.

6.3. Outbrain shall enter into appropriate contractual arrangements with its publishers or third party partners, requiring all parties to comply with Data Protection Laws.

6.4. Outbrain shall comply with requests from End Users to exercise their rights under relevant Data Protection Laws, without undue delay and within the required time limits. Requests relating to right to access, erasure, withdrawing consent, objecting to profiling, or "Do Not Sell My Personal Information" can be exercised directly on Outbrain Interest Profile.

6.5. To the extent that Outbrain receives and interprets consent strings or “Do Not Sell My Personal Information” strings as per Section 5.4, Outbrain is doing so in order to abide by an End User’s choice and shall not be deemed to be a Processor or Service Provider on anyone's behalf.

7. COOPERATION.

7.1. Each party shall develop, implement, and regularly review procedures to ensure they meet their respective obligations under Data Protection Laws.

7.2. Each party shall immediately inform the other party if any activity pursuant to the Agreement infringes any part of Data Protection Laws, and the parties shall review such activity accordingly. If during the term, Data Protection Laws change in a way that this DSA is no longer adequate for performing the processing activities necessary to the Terms, the parties agree to promptly negotiate in good faith to review this DSA in light of such changes.

7.3. In the event that either party receives any correspondence, enquiry or complaint from an End User, Supervisory Authority or any other third party related to the disclosure or processing of Personal Data pursuant to this DSA, or requests information from the other party when performing a Data Protection Impact Assessment, it shall promptly inform the other party giving full details of the same, and the other party shall provide such assistance as reasonably required (at each party’s sole cost and expense) and in good faith in order to respond in accordance with any requirements under Data Protection Laws.

8. DATA SECURITY.

8.1. Each party shall implement and maintain such appropriate technical and organizational measures as required by Data Protection Laws to ensure that the Personal Data is processed in a secure manner, including (but not limited to) (i) the pseudonymization and encryption of Personal Data; (ii) ensuring the confidentiality, integrity, availability and resilience of the services provided under the Agreement, including the ability to restore availability of, and access to, Personal Data in a timely manner in the event of a physical or technical incident; (iii) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing; and (iv) regularly carrying information security risk assessments that take account of risk of accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

8.2. An overview of Outbrain’s appropriate technical and organizational security measures are described on Outbrain’s Security page.

8.3. Upon becoming aware of a suspected or confirmed Personal Data Breach or Security Incident involving Outbrain Pixel Data collected pursuant to this DSA, each party shall notify the other party without any undue delay, and provide such assistance as reasonably required to allow the other party to comply with its respective obligations under Data Protection Laws.

9. PERSONNEL. Each party shall be responsible for ensuring that staff members are appropriately trained to handle and process the Personal Data in accordance with their internal technical and organizational security measures, where relevant, together with Data Protection Laws, and have entered into confidentiality agreements relating to the processing of Personal Data.

10. PROCESSORS – SERVICE PROVIDERS. Each party shall remain independently responsible for appointing its respective Processors and/or Service Providers in accordance with Data Protection Laws.

11. INTERNATIONAL TRANSFERS.

11.1. Insofar as Personal Data is collected from End Users located within the territory of the EEA or the UK by either party during the course of the Agreement, neither party shall process any Personal Data (nor permit any Personal Data to be processed) in a country outside of the EEA or the UK unless: (i) that country has been designated by the European Commission or the ICO (as applicable) as providing an adequate level of protection for Personal Data; or (ii) it has taken such measures as necessary to ensure the transfer is compliant with EU Data Protection Laws.

11.2. The parties agree that for the purposes of any transfer of Personal Data from Customer to Outbrain collected within the EEA to the UK, the requirements of the clause above shall be fully satisfied by the UK Adequacy Decision.

11.3. Outbrain shall be responsible for the onward transfer of Personal Data from the UK to any third party country outside of the EEA as required by (a) the UK Adequacy Decision and/or (b) EU Data Protection Laws, as applicable.

11.4. Within its Affiliates, Outbrain has entered into adequate intragroup data sharing agreements including supplementary measures complying with all requirements of EU Data Protection Laws, which consist of (i) encryption in transit; (ii) pseudonymization; and (iii) not having received any legally binding request from a public authority, including judicial authorities, under the laws of the country of destination and not being aware of any direct access by public authorities.

11.5. In the event that the UK Adequacy Decision as the lawful ground for international transfers from the EEA to third party countries is no longer applicable, the parties agree that the Controller SCCs shall be incorporated by reference into this DSA and shall govern any international transfer of Personal Data outside of the EEA. For the purpose of the Controller SCCs, the parties fully agree that:

(i) Customer is the "Data Exporter" and Outbrain, the "Data Importer";

(ii) Clause 7 “Docking clause” is deleted;

(iii) The OPTION under Clause 11 “Redress” is deleted;

(iv) Clause 17 “Governing Law” is completed with “Republic of Ireland”

(v) Clause 18 (b) “Choice of forum and jurisdiction” is completed with “Dublin, Republic of Ireland”;

(vi) Annex I to the Controller SCCs shall be deemed to have been completed with Annex I to this DSA; and

(vii) Annex II to the Controller SCCs shall be deemed to have been completed by Outbrain’s Security page.