Teads Advertiser Data Sharing Agreement

This Data Sharing Agreement ("DSA") is entered into by the company and/or Teads entity ("Company") and the individual or company (the "Customer") between the parties from time to time (together, the "Terms") and governs the processing of Personal Data pursuant to the provision of the Services by Company. This DSA shall apply to any and all agreements entered 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 EU SCCs (as applicable), the DSA, the Terms, and information entered or terms agreed, are together 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 EU 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.

1. DEFINITIONS.

1.1. "**Affiliate(s)**" means in respect of either party at any time, any person or legal entity controlled by or controlling or under the common control of that party. Any reference to the parties shall include reference to their Affiliates;

1.2. "**Controller EU SCCs**" means the standard data protection clauses "MODULE ONE: Transfer controller to controller" in accordance with article 46 2. (c) GDPR adopted by the European Commission on 4 June 2021 (Commission Implementing Decision (EU) 2021/914) (as amended or superseded), containing contractual obligations on the Data Exporter and the Data Importer, and rights for EEA Data Subjects whose Personal Data is transferred, as amended or superseded from time to time by the European Commission;

1.3. “**Controller UK Addendum**” means the international data transfer addendum to the European Commission’s standard contractual clauses for international data transfers issued under Section 119A of the Data Protection Act 2018 and following Parliamentary approval came into force on 21 March 2022;

1.4. “**CMP**” means an industry-standard consent management platform which enables the Customer to obtain, manage, and store End User’s Consent for the processing of Personal Data in compliance with Data Protection Laws;

1.5. “**Data Protection Laws**” means all applicable laws, guidance or codes of practice issued by a relevant public authority applicable from time to time to Company or Customer relating to the processing of Personal Data and the privacy of electronic communications, including U.S. Consumer Privacy Laws, EU and UK Data Protection Laws, the Brazilian General Data Protection Law (LGPD), Federal Law no. 13,709/2018 and the Japanese Act on the Protection of Personal Information;

1.6. “**Data Subject Rights**” means the exercise by a Data Subject or a Consumer of their rights under the Data Protection Laws;

1.7. “**EEA**” means the European Economic Area;

1.8. “**End Users**” means Data Subjects or Consumers who use the Service across the Network;

1.9. "**EU and UK Data Protection Laws**" means all laws, guidance or codes of practice issued by a relevant Supervisory Authority and the UK’s Commissioner applicable from time to time to Company or Customer relating to the processing of Personal Data and the privacy of electronic communications in the EEA and the UK as amended or superseded, especially (i) the General Data Protection Regulation ((EU) 2016/679) (GDPR) and the UK Data Protection Act 2018; (ii) UK GDPR (as defined in section 3(10) (as supplemented by section 205(4)) (iii) the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC) (ePrivacy Directive) and the UK Privacy and Electronic Communications Regulations 2003 (SI 2003 No. 2426) (PECR) as updated; (iv) the Swiss Federal Act on Data Protection 1992;

1.10. “**Company Pixel Data**” means the Personal Data which Company may collect when the Customer implements a pixel provided by Company (the “Company Pixel”) on Customer’s website(s) or application(s) for the purpose of providing measurement services related to Customer’s campaign(s), analytics related to the performance of the Customer’s campaign(s) and/or for enhanced targeting functionality;

1.11. “**Third Party Targeting**” means segments built independently by Customer or its third-party partners, which the Customer shares with Company for enhanced targeting of End Users;

1.12. “**UK Adequacy Decision**” means the Commission Implementing Decision of 28 June 2021 on the adequate protection of Personal Data by the United Kingdom in accordance with Article 45 GDPR;

1.13. “**U.S. Consumer Privacy Laws**” means all U.S. federal or state privacy laws, rules or regulations applicable from time to time to Company or Customer relating to the processing of Personal Data, including but not limited to, the California Consumer Privacy Act, the Colorado Privacy Act, the Connecticut Data Privacy Act, the Delaware Personal Data Privacy Act, the Iowa Consumer Data Protection Act, the Montana Consumer Data Privacy Act, Nebraska Data Privacy Act, the New Hampshire comprehensive privacy law, the New Jersey comprehensive privacy law, Oregon Consumer Privacy Act, Texas Data Privacy and Security Act, the Utah Consumer Privacy Act, the Virginia Consumer Data Protection Act, any applicable guidance or codes of practice issued by a relevant public authority, or any federal, state or national law, regulation or any self-regulatory or industry guidance;

1.14. "**Controller**", “**Consent**”, “**Joint Controller**”, "**Processor**", “**Data Protection Impact Assessment**”, "**Data Subject**", “**Personal Data Breach**”, "**Special Categories of Personal Data**", “**Commissioner**” and “**Supervisory Authority**” shall have the meanings given in EU and UK Data Protection Laws;

1.15. “**Business**”, “**Consumer**”, “**Controller**”, “**Cross-Context Behavioral Advertising** (including the targeting of advertising to a Consumer based on the Consumer’s Personal Information obtained from the Consumer’s activity across businesses, distinctly branded internet websites, applications, or services, other than the business, distinctly branded

internet website, application, or service with which the Consumer intentionally interacts)," "**Processor**" "**Sale**" (including the terms "sell," "selling," "sold," and other variations thereof, meaning the renting, disclosing, releasing, disseminating, making available, transferring, or otherwise communicating Personal Information for monetary or other valuable consideration), "**Service Provider**," "**Share**" (including the terms "shared," "sharing" and other variations thereof, meaning the renting, disclosing, releasing, disseminating, making available, transferring, or otherwise communicating of Personal Information by a Business to a Third Party for Cross-Context Behavioral Advertising), "T**argeted Advertising**" (including displaying advertisements to a Consumer where the advertisement is selected based on personal data obtained from that Consumer's activities over time and across nonaffiliated websites or online applications to predict such Consumer's preferences or interests) and "**Third Party**" shall have the meanings given to those terms under U.S. Consumer Privacy Laws, as applicable; and

1.16. "**Personal Data**" (and any variation thereof, including "Personal Information"), "**Sensitive Data**," "**Sensitive Personal Information**," and "**process**" (including "**processing**"), shall have the meaning given under the applicable Data Protection Laws.

2. U.S. CONSUMER PRIVACY LAWS AND EU AND UK DATA PROTECTION LAWS SPECIFIC PROVISIONS.

2.1. Specific provisions applicable to U.S. Consumer Privacy Laws are located in Sections 4.2, 5.3, 5.4.2, and 6.5.

2.2. Specific provisions applicable to EU and UK Data protection Laws are located in Sections 4.3, 5.4.1, 5.7, and 12.

3. PURPOSE OF PROCESSING. Where implemented by Customer, Company processes Company Pixel Data for the specific and limited purposes of providing aggregated analytics related to the performance of the Customer's campaign(s) and/or for enhanced targeting functionality, as disclosed by the IAB TCF Purposes 1, 3, 4, 7, 9 and 10. Each party shall remain solely and exclusively responsible for determining the means and

purposes of processing for its respective processing activities including complying with data protection principles under the Data Protection Laws. Each party shall assist the other with its compliance with data protection principles under the Data Protection Laws.

4. ROLE OF PARTIES.

4.1. Each party shall comply with all 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 U.S. Consumer Privacy Laws are applicable to the Service, Company shall be a Third Party to Customer as it relates to the processing, Sharing for Targeted Advertising and Selling of the Personal Data, and no party shall be considered a Service Provider or Processor on anyone's behalf. To the extent that the IAB Multi-State Privacy Agreement (the most recent version or successor thereto) ("MSPA") applies, it shall be incorporated by reference into this DSA and the relationship between Customer and Company shall be described in the MSPA. In the event of conflict between the MSPA and this DSA, the DSA shall prevail. The description of processing is described in Section B of Annex 1, attached hereto.

4.3. Insofar as EU and UK 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 the Company Pixel by Customer, and the parties shall be deemed independent Controllers for any other processing activity. The Customer shall be an independent controller for any Third-Party Targeting.

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 Pixels or Third Party Targeting: (i) for discriminatory purposes; (ii) to target minors under the age of eighteen (18); (iii) to target or collect Special Categories of Personal Data, Sensitive Data or Sensitive Personal Information; (iv) to collect Personal Data related to alleged or confirmed criminal convictions or offenses; or (v) in violation of any applicable law in any country the Customer is based or where the Campaign is displayed.

5.3. When implementing the Company Pixel on their website(s) or application(s) and/or utilizing Third Party Targeting, the Customer shall:

5.3.1. Disclose to End Users via a privacy notice that it complies with Data Protection Law and disclose that it uses Third Party Targeting and/or Pixels, including an explanation that Third Parties, including Company, may use cookies or other 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 3. Such privacy notice shall disclose to End Users, as applicable, the appropriate consent or opt out choice mechanism regarding the collection and disclosure of their Personal Data, including Company in compliance with applicable Data Protection Laws. Partner may also direct End Users to Teads Deactivated Personalised Ads link, accessible on Teads Privacy Policy, the Company opt out tool available here.

5.3.2. Insofar as EU and UK Data Protection Laws are applicable to the Service, use a consent management platform using the IAB Transparency & Consent Framework v2.2 (the most recent version or successor thereto) and pass Company valid "consent"/"no consent" strings after an End User has interacted with the consent management platform ("CMP"). Additionally, the Customer must ensure that the Company Pixel does not load before the End User has interacted with the CMP; or

5.3.3. Insofar as U.S. Consumer Privacy Laws are applicable to the Service, provide End Users with (i) a "Do Not Sell or Share My Personal Information" or "Your Privacy Choices" link in the footer of Customer's website(s) or application(s); (ii) an easily accessible mechanism to exercise their opt out rights through an opt out preference signal such as the Global Privacy Control; and/or (iii) an equivalent opt out choice using the IAB Global Privacy Platform (the most recent version or successor thereto) via a

CMP that passes Company valid “yes”/”no” strings after an End User has interacted with the CMP.

5.4. To the extent the Customer utilizes a CMP, it shall ensure that the CMP:

5.4.1. is compliant with Data Protection Laws, and any applicable guidance and/or industry best practices from regulatory or self-regulatory bodies.

5.4.2. clearly informs End Users about Company’s processing of Personal Data in accordance with Data Protection Laws (including by clearly mentioning Company in its list of vendors);

5.4.3. informs the End User about the purposes for which their Personal Data will be processed and allows End Users to provide Consent (to the extent required by Data Protection Laws) for specific processing purposes and manage preferences on a granular level, without bundling different processing purposes together;

5.4.4. informs the End User about the legal basis for such processing, and their rights in relation to their Personal Data;

5.4.5. obtains Consent from End Users (to the extent required by Data Protection Laws) that is freely given, specific, informed, and unambiguous indication of the End Users’ wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her;

5.4.6. provides a mechanism to allow End Users to select the option for consent including, “accept all”, “reject all” and/or “manage preferences” with all options being of equal prominence; and

5.4.7. prevents the End User from interacting with the Customer’s site(s) until such time as they have provided a consent indication.

5.5. In addition, the Customer shall:

5.5.1. provide a mechanism to allow End Users to withdraw their Consent (to the extent required by Data Protection Laws) at any time, and the withdrawal process must be at least as easy as the mechanism of providing Consent as per the Options;

5.5.2. prohibits the processing of Personal Data unless the End User has provided Consent (to the extent required by Data Protection Laws);

5.5.3. collect a clear, auditable record of the Consents (to the extent required by Data Protection Laws) given by End Users, including the date and time of Consent, the specific purposes for which consent was given, and any subsequent withdrawal of Consent; and

5.5.4. provide mechanisms for End Users to access, update, or delete their Consent preferences (to the extent required by Data Protection Laws) at any time.

5.6. Where the Customer does not use any of the above consent management platforms that permit an End User to opt out or withdraw their consent to personalized advertising, Targeted Advertising, and/or Cross-Contextual Behavioral Advertising via Customer's website(s) or Customer's application(s), Customer shall not load the Company Pixel.

5.7. Customer shall be responsible for ensuring that no more Personal Data than necessary is shared with Company via the Company Pixel.

5.8. Upon request, the Customer shall provide Company with all reasonable information to demonstrate compliance of the CMP with Data Protection Laws.

5.9. Where Company determines the CMP fails to comply with Data Protection Laws or is not present on the Customer's website(s) or application(s) where required, Company shall inform the Customer of such non-compliance and the Customer shall promptly and in any event within ten (10) working days implement any and all reasonable changes requested by the Company and shall notify the Company in writing of the actions taken to remediate any non-compliance of the CMP.

5.10. In the event the Customer fails to comply with Sections 5.7 through 5.9, Company at its discretion, reserves the right to either suspend its Services to the Customer or consider End User to have not provided its Consent.

5.11. Notwithstanding the foregoing, Customer acknowledges and agrees that Customer is solely responsible for its compliance obligations under Data Protection Laws.

6. COMPANY'S OBLIGATIONS.

6.1. Company shall:

6.1.1. 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.

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

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

6.1.4. 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 or Share My Personal Information" can be exercised directly to dpo@teads.com

6.2. Insofar as U.S. Consumer Privacy Laws are applicable to the Service, Company shall comply with the U.S. Consumer Privacy Laws, including treating Personal Data made available to Company by Customer in a manner consistent with Customer's obligations under the U.S. Consumer Privacy Laws. Company shall provide the same level of privacy protection for Personal Data made available to Company by Customer as is required of Customer under the U.S. Consumer Privacy Laws.

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 SUBJECT RIGHTS.

8.1. Each party is responsible for responding to Data Subject Rights received by the party. Company will assist Customer in fulfilling Data Subject Rights from End Users, as legally required. Each party agrees to provide such assistance as is reasonably required to enable the other party to comply with Data Subject Rights Request within the time limits imposed by the Data Protection Laws.

8.2. Data Subjects can exercise their rights directly via the Teads Deactivated Personalised Ads link, accessible on Teads Privacy Policy, and or by contracting our DPO at dpo@teads. Each party shall make the essence of this DSA available to Data Subjects in accordance with Data Protection Laws.

8.3. Each party is responsible for maintaining a record of Data Subject Rights Requests, the decisions made and any information that was exchanged. Records must include copies of the request for information, details of the data accessed and shared and where relevant, notes of any meeting, correspondence or phone calls relating to the request.

9. DATA SECURITY.

Each party shall:

9.1. 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. In the case of a Security Incident, the concerned party will take action as may be necessary to mitigate or remedy the effects of the Security Incident. When necessary, the party shall closely co-operate each other to assist in the investigation, mitigation, and remediation of such incident(s).

9.2. Each party shall implement the following security measures: (i) confidentiality (personal data will be stored and encrypted at rest using industry standard NIST-compliant algorithms; access to decryption keys will be strictly monitored and limited to runtime use online; anonymised data may be used for testing or debugging while ensuring confidentiality), (ii) access control (access to personal data systems will follow the principle of least privilege and be granted on a need-to-know basis; all access and data manipulation will be logged and monitored for at least 3 months; secrets and passwords will be securely stored (not in clear text), with user passwords complying with industry standardNIST 800-63B guidelines and renewed only if compromised; API keys and application secrets will meet minimum length requirements), (iii) segregation of data (personal data will be stored in dedicated datastores that are logically or physically separated from other systems, with separate service accounts; network-level segregation with whitelist filtering will prevent unauthorised access and limit breach impact), (iv) audit (all systems handling personal data will be regularly audited by independent third parties to ensure compliance with security best practices and these measures).

9.3. Upon becoming aware of a suspected or confirmed Personal Data Breach or Security Incident involving Company Pixel Data collected pursuant to this DSA, 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.

10. 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.

11. PROCESSORS – SERVICE PROVIDERS.

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

12. INTERNATIONAL TRANSFERS.

12.1. 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 UK's Commissioner (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 and UK Data Protection Laws.

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

12.3. Company 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 and UK Data Protection Laws, as applicable.

12.4. Within its Affiliates, Company has entered into adequate intragroup data sharing agreements including supplementary measures complying with all requirements of EU and UK Data Protection Laws, which consist of (i) encryption in transit and encryption of UUIDs at rest which can only be decrypted with a private key stored in the EU; (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.

12.5. 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 EU 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 EU SCCs, the parties fully agree that:

12.5.1. Customer is the "Data Exporter" and Company, the "Data Importer";

12.5.2. Clause 7 “Docking clause” is deleted;

12.5.3. The OPTION under Clause 11 “Redress” is deleted;

12.5.4. Clause 17 “Governing Law” is completed with “Republic of Ireland”

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

12.5.6. Annex I to the Controller EU SCCs shall be deemed to have been completed with Annex I to this DSA; and

12.5.7. Annex II to the Controller EU SCCs shall be deemed to have been completed by Company’s Security page.

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

12.6.1. Table 1: Parties Details: Customer is the "Data Exporter" and Company, the "Data Importer" with the start date, parties details, contact details and signature as set out in the Insertion Order;

12.6.2. Table 2: the selected SCCs are the Approved EU SCCs (Controller EU SCCs), including the Appendix Information and only with the following module, clauses or optional provisions of the Approved EU SCCs brought into effect for the purpose of this Controller UK Addendum:

12.6.2.1. Module: One - Controller to Controller;

12.6.2.2. Clause 7 “Docking clause” is deleted;

12.6.2.3. The OPTION under Clause 11 “Redress” is deleted;

12.6.2.4. Clause 17 “Governing Law” is completed with [“Republic of Ireland”]

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

12.6.3. Table 3: Appendix Information

12.6.3.1. Annex I to the Controller UK Addendum shall be deemed to have been completed with Annex I to this DSA; and

12.6.3.2. Annex II to the Controller UK Addendum shall be deemed to have been completed by Company’s Security page.

12.6.3.3. Annex III to the Controller UK Addendum: not applicable to Module One (Controller to Controller).

12.7. Table 4: Ending this Controller UK Addendum when the Approved Addendum changes: Importer.

13. TERM AND TERMINATION. This DSA shall commence on the Effective Date and shall continue as long as the Customer uses the Service.

14. DATA RETENTION. Company shall not retain any individual data point collected in relation to the Company Pixel for longer than 13 months, unless it constitutes anonymous data.

15. MISCELLANEOUS.

15.1. Neither party shall be in breach of this DSA nor liable for delay in performing, or failure to perform, any of its obligations under the Agreement if such delay or failure results from events, circumstances or causes beyond its reasonable control.

15.2. Failure or delay in exercising any right or remedy under this DSA shall not constitute a waiver of such (or any other) right or remedy under this DSA, the Agreement or Data Protection Laws.

15.3. Customer shall not assign or otherwise transfer its rights or its obligations under this Agreement, in whole or in part, without the prior written consent of Company.

15.4. Except as expressly stated otherwise and to the extent applicable under Data Protection Laws, nothing in this DSA shall create or confer any rights or other benefits in favor of any person other than a party to this DSA.

15.5. The invalidity, illegality, or unenforceability of any term of this DSA shall not affect the remainder of the DSA.

15.6. This DSA shall be governed by the laws specified in the Insertion Order.

ANNEX I

Description of Processing Activities

This Annex forms part of the DSA and describes the processing of Personal Data by Company. When Section 12.5 of the DSA applies, Annex I to the Controller EU SCCs shall be deemed to have been completed with this Annex.

A. LIST OF PARTIES

Data Exporter:

- Customer name, address and contact details as stated in the Applicable Principal Agreement.
- Activities relevant to the data transferred: Digital services or media delivered through a website or mobile application on which Customer has ownership and control.
- Joint Controller (collection whenever Company Pixel is implemented by Customer) and independent Controller (any other processing).

Data Importer:

- Company with address and contact details as stated in the Principal Agreement.
- Activities relevant to the data transferred: Digital advertising services.
- Joint Controller (collection whenever Company Pixel is implemented by Customer) and independent Controller (any other processing).

B. DESCRIPTION OF TRANSFER

- **Categories of Data Subjects whose Personal Data is transferred:** End Users (Data Subjects who visit or use Customer's website or application pages or interact with Customer's campaigns served by Company).
- **Categories of Personal Data transferred:**
    - Cookie ID
    - Mobile Advertising ID
    - IP Address
    - Non-precise Geolocation in our industry
    - Page URL and Mobile application information
    - Users interaction with Teads ads
    - Data and time
    - Browser information
    - Device information

    - Network type or mobile carrier information
- **Sensitive data transferred:** No Special Categories of Personal Data are transferred.
- **Frequency of the transfer:** Whenever Company Pixel is implemented and loaded on events determined by Customer, or whenever Customer shares Third Party Targeting with Company.
- **Nature of the processing:**
    - Receiving data, including collection, accessing, retrieval, recording, and data entry;
    - Holding data, including storage, organization and structuring;
    - Using data, including analyzing, consultation, testing, automated decision making and profiling;
    - Updating data, including correcting, adaptation, alteration, alignment and combination;
    - Protecting data, including restricting, encrypting, and security testing;
    - Sharing data, including disclosure, dissemination, allowing access or otherwise making available;
    - Returning data to the Data Exporter or Data Subject;
    - Erasing data, including destruction, deletion and anonymization.
- **Purpose(s) of the data transfer and further processing:** Digital advertising services, which include providing aggregated analytics related to the performance of the Customer's campaign(s) and/or for enhanced targeting functionality.
- **Retention period:** An individual data point is retained for no longer than 13 months from the date of collection.
- **Recipients:** The subject matter, nature and duration can be found on the Company Business Partners page.

C. COMPETENT SUPERVISORY AUTHORITY

- In the UK: The Information Commissioner's Office.

<u>Appendix:</u> TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

Teads and Teads' Affiliates will implement and maintain the following technical and organizational security measures:

Confidentiality

Personal data must always be an encrypted format, during network transit and at rest. Access to the decryption keys should be monitored for fraudulent access and should only be used by the service or application during run time. The encryption algorithms, modes, and key length should follow the NIST standard 800-175b.

Personal data may be stored in an anonymized way for testing purposes or debugging, provided that the anonymization procedure guarantees the confidentiality of information processed.

Access control

Access rules authorizing access to datastores or systems handling personal data should follow the principle of least privilege. These privileges should be assigned on a need to know basis. Access and manipulation of personal data should be monitored and logged

for a period allowing a potential investigation to construct an appropriate timeline of events.

Secrets and passwords used to access systems or datastores hosting personal data should never be stored in clear text, even in the application's source code. Appropriate measures should be taken in order to store secrets in a secure and reliable fashion.

User passwords should be compliant with the NIST 800-63B guidelines – minimum length of 8 characters and not follow obvious patterns (e.g. company123) or be dictionary word.

Renewal of passwords should only occur upon suspicion of a breach or leak of the password.

API keys and application secrets should be generated randomly.

Segregation of data

Personal data processed under this agreement should be stored in a dedicated datastore logically or physically separated from existing systems. By logically separate we mean: a dedicated database, or dedicated cluster or dedicated node, or system of nodes. The separation should extend to the service and application accounts querying the datastore. The breach of a datastore should not directly lead the breach of the datastore holding the data processed under this agreement.

Datastores and systems should be segregated from a network perspective from the rest of the internal network and be subject to a whitelist type of filtering.

Audit

All systems interacting either directly or indirectly with personal data should be regularly audited by a third party to ensure compliance with the security best practices and the aforementioned guidelines.