



## DATA PROTECTION ADDENDUM

### PREAMBLE

This Data Protection Addendum (the "**Addendum**") is entered into by and between TEADS SA, a company incorporated under the laws of Luxembourg whose principal place of business is at 5 rue de la Boucherie, L12 47 Luxembourg Paris, on behalf of itself and Teads Affiliates (defined below) (collectively, "**Teads**") and the undersigned counterparty ("**PARTNER**") on behalf of itself and its Affiliates (defined below), each a "**Party**" and collectively, the "**Parties**".

This Addendum amends the Principal Agreement that applies to the provision of Teads Service (as defined below) signed between the Parties (the "Principal Agreement").

The purpose of this Addendum is to define the respective responsibilities of the Parties for compliance with the obligations set out in EU Data Protection Law as defined below, in particular as regards the exercising of the rights of the data subjects.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Principal Agreement. Except where the context requires otherwise, references in this Addendum to the Principal Agreement are to the Principal Agreement as amended by, and including, this Addendum.

### 1. DEFINITION

1.1 In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1 "**Applicable Laws**" means (a) European Union or Member State laws with respect to any Personal Data; and (b) any other applicable law with respect to any Personal Data;

1.1.2 "**Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Partner, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

1.1.3 "**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.4 "**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); and (iv) any legislation replacing or updating any of the foregoing.

1.1.5 "**GDPR**" means EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 which is applicable from May 25<sup>th</sup>, 2018;



- 1.1.6 **“Teads Affiliates”** means an entity that is owned or controlled by Teads SA, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise. It is agreed that the Teads Affiliate is identified in the Principal Agreement.
- 1.1.7 **"Teads Services"** means the services and other activities to be supplied to or carried out pursuant to the Principal Agreement;
- 1.1.8 **“Users Personal Data”** means data that is collected by Teads through Teads web tags or mobile SDK on the Partner’s Properties which include user IP address, user ID that can be attributed to a user via cookies and other information sent by the user’s browser or user’s application such as page url, user agent, application name, device information or user interaction with ads;
- 1.1.9 **“Users”** means the end users visiting Partner Property(ies) and user viewing the ads on the Partner Property(ies).
- 1.1.10 **“Security Incident”** means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data of the other Party. For the avoidance of doubt, any Personal Data Breach of the other Party’s Personal Data will comprise a Security Incident
- 1.2 The terms, "Controller", "Data Subject", “Personal Data”, "Personal Data Breach", "Processing" and "Supervisory Authority" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.
- 1.3 The word "include" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.



## **2. SCOPE OF THE ADDENDUM**

- 2.1** Both Parties will jointly determine the purposes and means of the Processing of User Personal Data as described in Exhibit, in connection with the performance of each Party's obligations under the Principal Agreement for the purpose of monetizing the Partner's ad inventory through Teads platform and for the placement of ads. Therefore, the Parties agree that they will each act as a joint controller for the User Personal Data processing.
- 2.2** This Addendum only applies to the extent that EU Data Protection Law applies to the Processing of Personal Data, including if (a) the Processing is 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 by or on behalf of a Party. The Parties shall ensure that they will Process Personal Data solely for the purposes contemplated in the Principal Agreement, this Addendum or as otherwise agreed to in writing by the Parties. For the avoidance of doubt, this Addendum and the obligations hereunder do not apply to aggregated reporting or depersonalized statistics a Party may provide to the other Party in connection with the provision of the Services.

## **3. RESPECTIVE ROLES AND OBLIGATIONS OF THE PARTIES**

For the performance of their respective obligations, each Party considered as data controller shall, at all times, comply with their respective obligations pursuant to the GDPR.

### **3.1 For Partner**

The Partner warrants and undertakes to:

- (i) ensure that prior to any third party data collection on the Property(ies), the Users have been provided with appropriate information and choice mechanisms. The Partner should provide Users with easily accessible and comprehensive privacy policies and notices that are in compliance with GDPR, including relevant disclosures such as the descriptions of how data is collected, how that information is being used and how it affects the User's browsing experience, if data is being shared with third parties, and where Users can easily control their experience and exercise their rights.
- (ii) obtain from the Users legally valid consent to the processing of Users Personal Data for the purpose defined in the Exhibit and when seeking consent, the Partner must ensure to (a) retain records of consent given by Users; and (b) provide Users with clear instructions for revocation of the consent.
- (iii) without prejudice of the application of section 3.2.4, in case of Security Incident, the Partner shall proceed with a public communication on its Properties to inform Users and any relevant Data Subjects in an efficient way of the Personal Data Breach, where applicable and pursuant to article 34 of the GDPR.
- (iv) ensure to promptly redirect to Teads any request of access it directly receives from the Users or any Data Subject in relation to the performance of the Teads Services. Additionally, the Parties agree to monitor data protection enquiries as well as any Users and Data Subjects requests.



### **3.2 For Teads**

Teads will process User Personal Data according to the Principal Agreement, this Addendum and Exhibit. As joint controller, Teads undertakes to take in charge the following obligations:

- (i) Answer to Users and Data's Subjects requests regarding how Teads is processing the User Personal Data and comply with correction and deletion requests where applicable or technically feasible.
- (ii) Record in its registry the Personal Data processing implemented for the performance of the Teads Services in mentioning the existence of the joint control and making reference to this Addendum.
- (iii) Implement a maximum data retention policy for User Personal Data, set at 12 months.
- (iv) Implement appropriate technical and organizational measures to protect User Personal Data that is collected and processed for the performance of the Teads Services. In case of Security Incident, Teads will action measures as may be necessary to mitigate or remedy the effects of the Security Incident and will be in charge to report the Personal Data Breach under the EU Data Protection Law to the Supervisory Authority when legally required. Teads will also held a data breach registry as required by the GDPR. Partner shall closely co-operate with Teads to assist in the investigation, mitigation, remediation of such Personal Data Breach.
- (v) Conduct any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Teads considers to be required under articles 35 or 36 of the GDPR, in each case solely in relation to Processing of User Personal Data.
- (vi) Take into consideration, in terms of its tools, products, applications or services, the principles of data protection by design and by default.

### **3.3 Notifications**

For any notification between the Parties in relation to the fulfillment of their obligations listed above, each Party will define the point of contacts:

- For Teads: [dpo@teads.tv](mailto:dpo@teads.tv)

## **4. Liability**

Each party shall be liable to the other party for damages it causes by any breach of this Addendum. Liability as between the parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a party for its outrageous conduct) are specifically excluded. Each party shall be liable to Data Subjects for damages it causes by any breach of this Addendum.



Each Party agree to defend the other Party against any claim by a third party (including any Supervisory Authority, Users and/or any Data Subject) that is related to the other Party's breach of this Addendum. The breaching Party agrees to indemnify the other Party for settlement amounts or damages, liabilities, costs and expenses (including reasonable legal fees) awarded and arising out of such claims.

## **5. THIRD PARTY DATA PROCESSORS**

Each Party acknowledges that in the provision of the Teads Services, it may transfer Personal Data to and otherwise interact with third party data processors. Each Party agrees that if and to the extent such transfers occur, the transferring Party is responsible for entering into separate contractual arrangements with such third party data processors binding them to comply with obligations in accordance with Applicable Data Protection Law. For the avoidance of doubt, such third party data processors are not Subprocessors.

## **6. TERM**

The term of this Addendum will take effect on the date of execution of this Addendum by the Parties and will remain in effect until the Principal Agreement is terminated ("Effective Date"). The Parties agree that Users Personal Data will be processed by the other Party for the duration of the Services under the Agreement. Upon termination or expiry of this Addendum, each Party may continue to process Users Personal Data provided that such Processing complies with the requirements of this Addendum (12 months from the date of collection according to the Exhibit) and Applicable Data Protection Law. Notwithstanding the Effective Date of this Addendum, the Parties agree that the obligations under this Addendum that are specific to the GDPR shall not apply until the GDPR has come into full force and effect.

## **7. MISCELLANEOUS**

This Addendum and any underlying Agreement shall constitute the entire agreement between the Parties with respect to the subject matter hereof, and this Addendum supersedes all prior agreements or representations, oral or written, regarding such subject matter including any provisions in the Agreement which address the processing of Personal Data.

This Addendum and all disputes arising out of or relating to this Addendum shall be interpreted, construed and enforced in accordance with French law. Each Party irrevocably consents to the exclusive jurisdiction of the courts situated in France over all such disputes and claims under this Addendum and all actions to enforce such claims or to recover damages or other relief in connection with such claims under this Addendum except to the extent that Applicable Data Protection Law requires otherwise.

The Parties shall agree that electronic format shall be deemed an acceptable means of communication in the execution or sending of an addition or modification to the terms of this Addendum.

Any changes can only be made if both Parties are in agreement. The summary of this Addendum will be made public on the Partner website to demonstrate an open and transparent approach regarding personal data protection.



**EXHIBIT 1  
DETAILS OF PROCESSING ACTIVITIES**

<p><b>Purposes of the Personal Data processing by Teads</b></p> <p><i>(Teads is using the purposes as defined by the IAB transparency and consent framework)</i></p>	<p><b>Storage and access of information:</b> The storage of information, or access to information that is already stored, on your device such as accessing advertising identifiers and/or other device identifiers, and/or using cookies or similar technologies.</p> <p><b>Personalization:</b> The collection and processing of information about your use of this site to subsequently personalize advertising for you in other contexts, i.e. on other sites or apps, over time. Typically, the content of the site or app is used to make inferences about your interests which inform future selections.</p> <p><b>Ad selection, delivery, reporting:</b> The collection of information, and combination with previously collected information, to select and deliver advertisements for you, and to measure the delivery and effectiveness of such advertisements. This includes using previously collected information about your interests to select ads, processing data about what advertisements were shown, how often they were shown, when and where they were shown, and whether you took any action related to the advertisement, including for example clicking an ad or making a purchase.</p> <p><b>Content selection, delivery, reporting:</b> The collection of information, and combination with previously collected information, to select and deliver content for you, and to measure the delivery and effectiveness of such content. This includes using previously collected information about your interests to select content, processing data about what content was shown, how often or how long it was shown, when and where it was shown, and whether the you took any action related to the content, including for example clicking on content.</p> <p><b>Measurement;</b> The collection of information about your use of the content, and combination with previously collected information, used to measure, understand, and</p>
--	---

	report on your usage of the content.
<b>Purposes where Users consent is required to be collected by the Partner</b>	<ul style="list-style-type: none"> <li>- Storage and access of information</li> <li>- Personalization</li> </ul>
<b>Purposes where Teads is relying on Teads legitimate interest</b>	<ul style="list-style-type: none"> <li>- Ad selection, delivery, reporting</li> <li>- Content selection, delivery, reporting.</li> <li>- Measurement</li> </ul>
<b>Categories of data subjects</b>	End users visiting the Partner Property(ies) and users viewing the ads on the Partner Property(ies).
<b>Types of personal data</b>	User Personal Data as defined here above in the Addendum.
<b>Data Recipients</b>	<ul style="list-style-type: none"> <li>- Teads.</li> <li>- The service providers selected by Teads such as the following categories: cloud services, fraud detection, ad verification, reporting. This includes for example Amazon Web Services, Moat, Integral Ad Science, Double Verify.</li> <li>- Demand Side Platforms.</li> </ul>
<b>EU data transfer</b>	No transfer outside EU.
<b>Retention period</b>	12 months from the collection.
<b>Where possible, a general description of the technical and organizational security measures</b>	<ul style="list-style-type: none"> <li>- Pseudonymization</li> <li>- Encryption of personal data</li> <li>- Access control</li> <li>- Security policy</li> <li>- Security auditing</li> </ul>