Data Processing Addendum

This Data Processing Addendum ("**DPA**") supplements the Contract between Tagboard ("**Processor**") and Customer ("**Controller**") (jointly the "**Parties**"), and applies when the GDPR applies to Controller's use of Processor's Services to Process Personal Data. Except as amended by this DPA, the Contract will remain in full force and effect. If there is a conflict between the Contract and this DPA, the terms of this DPA will control. Capitalized terms not defined in this DPA shall have the meaning given to them in the Contract.

1. **Definitions and Interpretation**.

1.1. Unless otherwise defined herein, capitalized terms and expressions used in this DPA shall have the following meaning:

1.1.1. "**Cessation Date**" has the meaning ascribed to it in Section 9.

1.1.2. "**Confidential Information**" has the meaning ascribed to it in Section 12.1.

1.1.3. "**Controller**" means the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

1.1.4. "**Data Protection Legislation**" means the GDPR and any applicable national implementing laws, regulations, and secondary legislation, as amended or updated from time to time, in the European Union.

1.1.5. "**Data Subject**" means an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular 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.

1.1.6. "**European Commission**" means the executive branch of the European Union.

1.1.7. "**GDPR**" means EU General Data Protection Regulation 2016/679.

1.1.8. "**Data Transfer**" means any transfer of Personal Data subject to this DPA: (a) from Controller to Processor; or (b) from Processor to a Subprocessor, where such transfer is from the European Economic Area to a third country that has not received an adequacy decision under Article 45 of the GDPR.

1.1.9. "**Personal Data**" means any information relating to a Data Subject.

1.1.10. "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed.

1.1.11. “**Processing**” means 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, organization, structuring, storage, adaptation, or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

1.1.12. “**Processor**” means the entity which Processes Personal Data on behalf of the Controller.

1.1.13. “**Services**” means all Tagboard provided services and products as further described in the Contract.

1.1.14. “**Standard Contractual Clauses**” means the standard contractual clauses for the transfer of personal data to processors established in third countries (Controller-to-Processor transfers) as approved by European Commission Decision 2021/914 of 4 June 2021, as may be amended, superseded, or replaced from time to time.

1.1.15. “**Subprocessor**” means any person appointed by or on behalf of Processor to process Personal Data on behalf of Controller in connection with the Contract.

1.1.16. “**Supervising Authorities**” means the independent public authorities established by an EU Member State pursuant to Article 51 of the GDPR to monitor and enforce compliance with the GDPR, and any other competent data protection authority responsible for monitoring compliance with Data Protection Legislation.

2. **Processing of Personal Data**.

2.1. Processor shall:

2.1.1.comply with all applicable Data Protection Legislation in the Processing of Personal Data; and

2.1.2.process Personal Data only as necessary to provide the Services selected and configured by Controller.

2.2. Controller selects which Services to use and determines the purposes for which Personal Data will be collected through those Services. Processor provides the Services using its standardized technical infrastructure and processes as described in the Contract. By selecting, configuring, and using the Services, Controller instructs and authorizes Processor to Process Personal Data accordingly.

2.3. For purposes of this DPA, including the Standard Contractual Clauses referenced in Section 11.2:

2.3.1.Subject Matter of Processing: The subject matter of Processing is the provision of the Services under the Contract, including social media content aggregation, curation, display, moderation, and analytics services based on social media accounts of Controller’s end users, as well as interactive audience engagement features such as QR code-enabled polls, trivia, and content sharing functionality.

2.3.2. Duration of Processing: Processor will Process Personal Data for the duration of the Contract, including any renewal periods, and for up to 30 days thereafter as set forth in Section 9.

2.3.3. Nature and Purpose of Processing: Processor will Process Personal Data for the purpose of providing the Services to Controller as selected, configured, and instructed by Controller. This includes collecting and aggregating content from social media accounts of Controller’s end users, storing and displaying such content, enabling content moderation, and providing analytics. Additionally, Processor collects Personal Data through interactive features including QR code-based audience engagement tools (polls, trivia questions, and user-generated content sharing) for the purposes of facilitating audience participation, communication with end users, and analytics.

2.3.4. Types of Personal Data: The types of Personal Data processed may include social media usernames and handles, profile pictures and avatars, user-generated content, user-submitted photos and images, metadata associated with social media posts (such as timestamps and location tags), social media account credentials or authentication tokens, IP addresses, device identifiers, names, email addresses, phone numbers, and geolocation data (limited to city-level information).

2.3.5. Categories of Data Subjects: The categories of Data Subjects whose Personal Data may be processed include Controller’s end users, including Controller’s end users who participate in interactive features such as polls, trivia, or content sharing, individuals whose content appears in Controller’s end user’s social media accounts, Controller’s end users who view or interact with content through the Services, and Controller’s authorized personnel who access and use the Services.

3. Processor Personnel. Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Processor or Subprocessor who may have access to Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Personal Data, as strictly necessary for the purposes of the Contract, and to comply with applicable laws in the context of that individual's duties to Processor or the Subprocessor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality. Processor shall ensure that all personnel authorized to process Personal Data have received appropriate training on data protection obligations and the requirements of this DPA.

4. **Security**.

4.1. Taking into account the available technology, the costs of implementation, and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall in relation to the Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2. In assessing the appropriate level of security, Processor shall take account the risks that are presented by Processing, in particular from a Personal Data Breach.

4.3. Processor shall maintain reasonable security practices appropriate to the nature and scope of Processing, including: (a) procedures for identifying, assessing, and applying security updates and patches based on risk and criticality; (b) regular security testing, including vulnerability assessments, with frequency and scope determined by Processor's risk assessment; (c) security monitoring capabilities to detect and respond to security incidents; and (d) documentation of security policies and procedures sufficient to demonstrate compliance with this DPA.

4.4. Controller may request information regarding Processor's security measures no more than once per twelve-month period (unless required by law or in response to a suspected or actual Personal Data Breach). Processor shall respond to reasonable requests within thirty (30) days. Controller's audit and inspection rights are set forth in Section 10.

5. **Subprocessing**.

5.1. Customer provides Tagboard general written authorization to engage Subprocessors to process Personal Data on Customer’s behalf. The Subprocessors engaged by Tagboard are listed at: https://support.tagboard.com/knowledge-base/sub-processors-and-subcontractors.

5.2. Tagboard shall provide Customer with at least 10 days’ advance notice (email being sufficient) of the addition or replacement of any Subprocessor by updating the list referenced in Section 5.1 and sending notice to Customer’s email address on file. Customer may object to the engagement of a new or replacement Subprocessor within 10 days of such notice, provided the objection is based on reasonable data protection grounds.

5.3. If Customer does not object within the 10-day notice period, Customer shall be deemed to have authorized the new or replacement Subprocessor. If Customer reasonably objects, Tagboard may, at its option: (a) not engage the objected-to Subprocessor; or (b) work with Customer to address the objection on commercially reasonable terms. If the Parties cannot reach resolution within 30 days, Customer's sole remedy shall be to terminate the affected Services by providing written notice to Tagboard, without penalty, and receive a pro-rata refund of prepaid fees for the terminated Services.

5.4. Notwithstanding Section 5.2, Tagboard may engage new Subprocessors on an emergency basis where reasonably necessary to prevent service disruption or address a security incident, provided Tagboard notifies Customer within 2 business days and Customer retains the objection rights set forth in Sections 5.2 and 5.3.

5.5. Tagboard shall ensure that each Subprocessor is bound by written obligations consistent with Tagboard's obligations under this DPA, provided that Tagboard may engage Subprocessors pursuant to such Subprocessor's standard terms of service where such terms provide data protection obligations that comply with applicable Data Protection Legislation. Tagboard shall remain fully liable to Customer for the Subprocessor's performance.

6. **Data Subject Rights**.

6.1. Taking into account the nature of the Processing, Processor shall assist Controller by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of Controller obligations, as reasonably understood by Controller, to respond to requests to exercise Data Subject rights under the Data Protection Legislation.

6.2. Processor shall:

6.2.1. Notify Controller within 5 business days if it receives a request from a Data Subject under any Data Protection Law in respect of Personal Data;

6.2.2. Ensure that it does not respond to that request except on the documented instructions of Controller or as required by applicable laws to which the Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws inform Controller of that legal requirement before the Processor responds to the request; and

6.2.3. Respond to Controller's reasonable requests for assistance under Section 6.1 within 10 business days of receiving such request, or such shorter period as reasonably necessary to enable Controller to comply with applicable statutory deadlines under Data Protection Legislation, provided that Controller gives Processor reasonable notice of any such shortened timeframe.

6.3. Controller shall reimburse Processor for reasonable costs incurred in providing assistance under this Section 6, including but not limited to costs associated with retrieving, compiling, or delivering Personal Data in response to data subject requests. Processor shall provide Controller with reasonable advance notice of anticipated costs where practicable.

7. **Personal Data Breach**.

7.1. Processor shall notify Controller within 48 hours of becoming aware of a Personal Data Breach affecting Personal Data. The notification shall include, to the extent reasonably available to Processor at the time: (a) a description of the nature of the breach; (b) the categories and approximate number of Data Subjects and Personal Data records affected; (c) the likely consequences of the breach; and (d) measures taken or proposed to address the breach and mitigate its potential adverse effects.

7.2. Processor shall reasonably assist Controller in meeting Controller's obligations under Data Protection Legislation to report the Personal Data Breach to Supervising Authorities or notify affected Data Subjects, including by providing additional information about the breach that becomes available after the initial notification under Section 7.1.

7.3. Processor shall cooperate with Controller and, to the extent legally required or as reasonably directed by Controller, with applicable data protection authorities in connection with any investigation or inquiry related to a Personal Data Breach. Processor shall take commercially reasonable steps directed by Controller to assist in the investigation, mitigation, and remediation of the breach.

7.4. Processor shall maintain documentation of all Personal Data Breaches, including the facts relating to the breach, its effects, and remedial actions taken, as required by Article 33(5) of the GDPR. Processor shall make such documentation available to Controller upon reasonable request.

8. **Data Protection Impact Assessment and Prior Consultation**. Processor shall provide reasonable assistance to Controller with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Controller reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Personal Data by, and taking into account the nature of the Processing and information available to, the Subprocessors.

9. **Deletion or Return of Personal Data**. Subject to this Section 9, Processor shall delete and procure the deletion of all copies of Personal Data within 30 days of the date of cessation of any Services involving the processing of Personal Data (the "**Cessation Date**"). Processor does not retain backup copies of any Personal Data. Processor will not use or otherwise process Personal Data except as strictly necessary to effectuate deletion and provide the Services under the Contract. The 30-day deletion period accounts for the technical requirements of Processor's data storage architecture.

10. **Audit Rights**.

10.1. Subject to this Section 10, Processor shall make available to Controller on request all information necessary to demonstrate compliance with this DPA, and shall allow for and contribute to audits, including inspections, by Controller or an auditor mandated by Controller in relation to the Processing of the Personal Data by the Subprocessors.

10.2. Information and audit rights of Controller only arise under section 10.1 to the extent that the DPA does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

11. **Data Transfer and Storage**.

11.1. Customer acknowledges and agrees that Processor may transfer and process Personal Data in the United States, where Processor's service infrastructure is located.

Personal Data will be stored on Processor's servers for up to 30 days as part of Processor's standard data retention and processing operations.

11.2. To the extent any transfer of Personal Data under this DPA is subject to the GDPR and is to a country that has not been subject to an adequacy decision by the European Commission, the parties agree that such transfer shall be governed by the Standard Contractual Clauses for the transfer of personal data to processors established in third countries (Controller-to-Processor transfers) as approved by the European Commission (the "**Standard Contractual Clauses**"), which are incorporated into this DPA by reference and shall be deemed executed by the Parties. For purposes of the Standard Contractual Clauses, Controller is the data exporter and Processor is the data importer, and the details of the processing activities are as set forth in Section 2.3 of this DPA.

11.3. If Processor becomes aware that it can no longer comply with its obligations under this DPA or the Standard Contractual Clauses due to changes in applicable laws, government access demands, or changes to Subprocessor policies or practices, Processor shall promptly notify Customer and, if necessary, suspend processing or permit Customer to terminate the affected Services in accordance with the terms of the Standard Contractual Clauses.

12. **General Terms**.

12.1. Confidentiality. Each Party must keep any information it receives about the other Party and its business in connection with this DPA ("**Confidential Information**") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

12.1.1. Such disclosure is necessary for the performance of this DPA; or

12.1.2. Such disclosure is made to employees, agents, or Subprocessors who have a need to know and are bound by confidentiality obligations at least as protective as those set forth in this DPA.