Data Processing Agreement

in accordance with Article 28 General Data Protection Regulation (GDPR)

Agreement

between

_____

– the Controller – hereinafter referred to as the Client -

and

EventMobi GmbH, Kopernikus Str. 35, 10243 Berlin, Germany

– the Processor - hereinafter referred to as the Supplier

[If applicable: Authorised Representative in accordance with Article 27 of the GDPR:

_____]

1. Subject matter and duration of the order or contract

(1) Subject matter

The Supplier provides a software and server infrastructure enabling communication between the event coordinator and the participant. Additionally, the Supplier runs an online platform facilitating the creation, maintenance and updating as well as management, planning and execution of event registrations or event live polls. The Supplier's clients are able to add and manage data manually. By providing the above services, the Supplier collects and/or processes and/or uses the client's data in accordance with the client's instructions according to Art. 28 para. 3 of the GDPR (data processing). With regard to data protection, the client is the controller owning the data. This contract depends on the user agreement.

(2) Duration

The duration of this contract depends on the user agreement. This does not prejudice the right to termination of the contract without notice.

2. Specification of the order or contract details

(1) Nature and purpose of the intended processing of data

Nature and purpose of processing of personal data by the Supplier for the Client are precisely defined in the user agreement.

The undertaking of the contractually agreed processing of data shall be carried out exclusively within a Member State of the European Union (EU) or within a Member State of the European Economic Area (EEA). Each and every transfer of data to a state which is not a Member State of either the EU or the EEA requires prior agreement of the Client and shall only occur if the specific conditions of Article 44 et seq. of the GDPR have been fulfilled.

(2) Categories of personal data

- General individuals' information (name, address)
- Contact details (telephone number, email address)
- Role of the individual in the company (e. g. department, responsibilities)
- Contract payment details (e. g. payment of registration fee)
- Links to social media profiles (e. g. Facebook, LinkedIn, Twitter)
- Biography or brief description (e. g. details on the career, skills)
- Contract details (e. g. contract relations, interest in products)
- Client history (e. g. attendance at previous events, interests)
- Payment details (e. g. time of payment, payment amount)
- Information from third parties (e. g. credit agencies, public directories)
- Technical data to ensure data transmission (e. g. IP address, device ID)

(3) Categories of data subjects

- Attendees and speakers at events organized by client
- Contractors of client
- Clients of client
- Potential clients of client
- Subscribers of client
- Employees of client
- Representatives of client
- Contact persons of client
- Potential attendees of events organized by client
- Individuals downloading the app of client without belonging to any of the categories of data subjects mentioned above

3. Technical and Organisational Measures

(1) Before the commencement of processing, the Supplier shall document the execution of the necessary technical and organisational measures set out in advance of the placement of the order or contract, specifically with regards to the detailed execution of the contract, and shall present these documented measures to the Client for inspection. Upon acceptance by the Client the documented measures become the foundation of the contract. Insofar as the inspection/audit by the Client shows the need for amendments such amendments shall be implemented by mutual agreement.

(2) The Supplier shall establish the security in accordance with Article 28 Paragraph 3 Point c), and Article 32 of the GDPR in particular in conjunction with Article 5 Paragraph 1, and Paragraph 2 of the GDPR. The measures to be taken are measures of data security and measures guaranteeing a protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems. The state of the art, implementation costs, the nature, scope and purposes of processing as well as the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 Paragraph 1 of the GDPR must be taken into account [Details in Appendix 1].

(3) The technical and organisational measures are subject to technical progress and further development. Bearing this in mind, it is permissible for the Supplier to implement alternative adequate measures. However, the security level of the defined measures must not be reduced. Substantial changes must be documented.

4. Rectification, restriction and erasure of data

(1) The Supplier may not on its own authority rectify, erase or restrict the processing of data that is being processed on behalf of the Client but only on documented instructions from the Client. If a data subject contacts the Supplier directly concerning a rectification, erasure, or restriction of processing the Supplier will immediately forward the data subject's request to the Client.

(2) If it is included in the scope of services the erasure policy, 'right to be forgotten', rectification, data portability and access shall be ensured by the Supplier in accordance with documented instructions from the Client without undue delay.

5. Quality assurance and other duties of the Supplier

In addition to complying with the rules set out in this contract the Supplier shall comply with the statutory requirements referred to in Articles 28 to 33 of the GDPR; accordingly, the Supplier ensures, in particular, compliance with the following requirements:

a) Designated Data Protection Officer performing his duties in compliance with Articles 38 and 39 of the GDPR is:
Kemal Webersohn
WS Datenschutz GmbH
Meinekestr. 13
10719 Berlin
Germany

Contact details are:
Telephone: +49 30 88 72 07 88
E-Mail: eventmobi@ws-datenschutz.de

The Client shall be informed immediately of any change of Data Protection Officer.

b) Confidentiality in accordance with Article 28 Paragraph 3 Sentence 2 Point b), Articles 29 and 32 Paragraph 4 of the GDPR. The Supplier entrusts only such employees with the data processing outlined in this contract that have been bound to confidentiality and have previously been familiarised with the data protection provisions relevant to their work. The Supplier and any person acting under its authority who has access to personal data shall not process said data unless on instructions from the Client which includes the powers granted in this contract unless required to do so by law.

c) Implementation of and compliance with all technical and organisational measures necessary for this order or contract in accordance with Article 28 Paragraph 3 Sentence 2 Point c), Article 32 of the GDPR [Details in Appendix 1].

d) The Client and the Supplier shall cooperate, on request, with the supervisory authority in performance of its tasks.

e) The Client shall be informed immediately of any inspections and measures conducted by the supervisory authority if they relate to this order or contract. This also applies if the Supplier is under investigation or is party to an investigation by a competent authority in connection with infringements to any Civil or Criminal Law, or administrative rule or regulation regarding the processing of personal data in connection with the processing of this order or contract.

f) If the Client is subject to an inspection by the supervisory authority, an administrative or summary offence or criminal procedure, a liability claim by a data subject or by a third party or any other claim in connection with the order or contract data processing by the Supplier the Supplier shall make every effort to support the Client.

g) The Supplier shall periodically monitor the internal processes and the technical and organizational measures to ensure that processing within his area of responsibility is in accordance with the requirements of applicable data protection law and the protection of the rights of the data subject.

h) Verifiability of the technical and organisational measures conducted by the Client as part of the Client's supervisory powers referred to in item 7 of this contract.

6. Subcontracting

(1) Subcontracting for the purpose of this agreement is to be understood as meaning services which relate directly to the provision of the principal service. This does not include ancillary services, such as telecommunication services, postal/transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment. The Supplier shall, however, be obliged to make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the data protection and the data security of the Client's data, even in the case of outsourced ancillary services.

(2) The Supplier may commission subcontractors (additional contract processors) only after prior explicit written or documented consent from the Client.

The Client agrees to the commissioning of the following subcontractors on the condition of a contractual agreement in accordance with Article 28 paragraphs 2-4 of the GDPR:

Company subcontractor	Address/country	Service
5TouchSolutions, Inc.	#400 207 Queens Quay W Toronto, ON M5J 1A7 Canada	Provision, maintenance and running of EventMobi's software

(3) Outsourcing to additional subcontractors and Changing the existing subcontractor is permitted if:

- The Supplier submits such an outsourcing to a subcontractor to the Client in writing or in text form with appropriate advance notice; and
- the Client has not objected to the planned outsourcing in writing or in text form by the date of handing over the data to the Supplier; and
- the subcontracting is based on a contractual agreement in accordance with Article 28 paragraphs 2-4 of the GDPR.

(4) The transfer of personal data from the Client to the subcontractor and the subcontractors commencement of the data processing shall only be undertaken after compliance with all requirements has been achieved.

(5) If the subcontractor provides the agreed service outside the EU/EEA, the Supplier shall ensure compliance with EU Data Protection Regulations by appropriate measures. The same applies if service providers are to be used within the meaning of Paragraph 1 Sentence 2.

(6) Further outsourcing by the subcontractor requires the express consent of the Supplier (at the minimum in text form).

All contractual provisions in the contract chain shall be communicated to and agreed with each and every additional subcontractor.

7. Supervisory powers of the Client

(1) The Client has the right, after consultation with the Supplier, to carry out inspections or to have them carried out by an auditor to be designated in each individual case. It has the right to convince itself of the compliance with this agreement by the Supplier in his business operations by means of random checks, which are ordinarily to be announced in advance.

(2) The Supplier shall ensure that the Client is able to verify compliance with the obligations of the Supplier in accordance with Article 28 of the GDPR. The Supplier undertakes to give the Client the necessary information on request and, in particular, to demonstrate the execution of the technical and organizational measures.

Evidence of such measures concerning not only the specific or contract may be provided by current auditor's certificates, reports or excerpts from reports provided by independent bodies (e.g. auditor, Data Protection Officer, IT security department, data privacy auditor, quality auditor).

(3) The Supplier may claim remuneration for enabling Client inspections.

8. Communication in the case of infringements by the Supplier

(1) The Supplier shall assist the Client in complying with the obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments and prior consultations, referred to in Articles 32 to 36 of the GDPR. These include:

a) Ensuring an appropriate level of protection through technical and organizational measures taking into account the circumstances and purposes of the processing as well as the projected probability and severity of a possible infringement of the law as a result of security vulnerabilities and enabling an immediate detection of relevant infringement events.
b) The obligation to report a personal data breach immediately to the Client.
c) The duty to assist the Client with regards to the Client's obligation to provide information to the Data Subject concerned and to immediately provide the Client with all relevant information in this regard.
d) Supporting the Client with its data protection impact assessment.
e) Supporting the Client with regards to prior consultation of the supervisory authority.

(2) The Supplier may claim compensation for support services not included in the description of the services and not attributable to failures on the part of the Supplier.

9. Authority of the Client to issue instructions

(1) The Client shall immediately confirm oral instructions (at the minimum in text form).

(2) The Supplier shall inform the Client immediately if he considers that an instruction violates Data Protection Regulations. The Supplier shall then be entitled to suspend the execution of the relevant instructions until the Client confirms or changes them.

10. Deletion and return of personal data

(1) Copies or duplicates of the data shall never be created without the knowledge of the Client, with the exception of back-up copies as far as they are necessary to ensure orderly data processing, as well as data required to meet regulatory requirements to retain data.

(2) After conclusion of the contracted work, or earlier upon request by the Client, at the latest upon termination of the Service Agreement the Supplier shall hand over to the Client or – subject to prior consent – destroy all documents, processing and utilization results, and data sets related to the contract that have come into its possession in a data-protection compliant manner. The same applies to any and all connected test, waste, redundant and discarded material. The log of the destruction or deletion shall be provided on request.

(3) Documentation which is used to demonstrate orderly data processing in accordance with the order or contract shall be stored beyond the contract duration by the Supplier in accordance with the respective retention periods. It may hand such documentation over to the Client at the end of the contract duration to relieve the Supplier of this contractual obligation.

_____

Date

_____

Signature of Controller

_____

Date

_____

Signature of Processor

Appendix 1
Technical and Organisational Measures

1. Physical Access Control

- No unauthorised access to data processing facilities
- Premises secured by access with keys
- Documentation of distribution of keys
- Repossession/Revocation of access after expiration of user rights

2. Access Control to Systems Processing Personal Data

- Password guideline
- Clean Desk Policy requiring all employees to dispose of documents according to requirements of the GDPR and to lock their devices when leaving the desk
- Encryption of data storage devices
- Installation of firewall, virus scanner, interface security
- Instructions for allocation of keys
- Immediate revocation of rights of leaving employees
- Copies are immediately encrypted
- Security concept is in place
- Technical and organisational measures ensure that necessary rights are revoked in a timely manner

3. Control of Access Rights

- Binding back up strategy
- Individual allocation of rights (e. g. profiles, roles)
- Administrative strategy in place for a comprehensive request and allocation of access rights
- Allocation of minimal access rights only

4. Separation Control

- Separation of production and testing environment by content
- Physical separation of systems, databases, data storage devices
- Client-capability of applications and software
- Allocation of rights with the help of access right strategy
- Specification of database rights
- Data with attributes

5. Transport Control

- Procedure for a GDPR-appropriate deletion/disposal of data storage devices and documents is in place
- Secured transport protocol (SSL, TLS, SFTP)
- Use of private data storage devices prohibited
- Instructions for the use of mobile data storage devices

6. Input Control

- Monitoring of user and time of specific changes made in the system
- Organisational specifications of responsibilities of an individual's rights to make changes in the system are documented.
- Every employee has the necessary access to data according to their role and in order to fulfil their work contract (Concept of Minimal Rights)
- Rights to access sensitive resources are comprehensively requested and allocated by individuals authorised to do so
- There is an input history for all users with access to personal data monitoring which individual performed which action at what point of time if personal data is modified.

7. Processing Control

- Control of contract performance
- The contract contains detailed information on the purpose of the controller's personal data as well as the prohibition of use of the personal data by the processor not specified in the contract
- The contract contains detailed information on the nature of the data processing and the use of personal data by the controller
- The processor designated a data protection officer and ensures appropriate and effective involvement in relevant operational processes
- Data Processing Agreements are in place with all other relevant processors
- A comprehensive order procedure is in place including the existence of an offer and order
- Placing an order is a formalised procedure (form)
- A general security concept is in place
- All employees with access rights have committed themselves to confidentiality in written form
- All employees received instructions/guidelines/leaflets giving information on measures implemented to ensure a security of data as well as IT security
- If an error occurs with regards to the processing of data or if the processor becomes aware of a personal data breach they will inform the controller immediately

8. Availability Control

- Back up strategy
- Mirroring of hard drives
- Installation of security programs (Firewall, SPAM filter, virus protection)
- Automated standard procedure for regular update of security software (Virus scanner, malware protection, firewall system)
- Redundant locations

9. Operational Control

- All employees with access rights have been informed about data security and have committed themselves to confidentiality in written form

- All employees are taught about data security at the workplace regularly (at least once a year)
- Regular audit by data protection officer
- Specified organisation of representatives within a department/organisation
- Procedure in place for regular audits, assessments and evaluation

10. Privacy by Default/Privacy by Design

- No more data than necessary to provide the service is processed
- Consent withdrawal for data subjects simplified with the use of technical and organisational measures