Data Processing Agreement

The following Data Processing Agreement (DPA) within the meaning of Art. 28 (3) GDPR governs the obligations and rights under data protection law in connection with the use of the platform of EventMobi GmbH between:

The controller (Art. 4 (7) GDPR) of data processing:

(Company)

(Address)

hereinafter referred to as the: controller

and the processor (Art. 4 (8) GDPR):

EventMobi GmbH

c/o WeWork, Warschauerplatz 11-13

10245 Berlin

Deutschland *hereinafter referred to as the: processor*

The content complies with the Commission's standard contractual clauses according to Art. 28 (6), (7) GDPR of 04.06.2021 (C 2021) 3701 final.

Table of contents

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29 (3) and (4) Regulation (EU) 2018/1725.

c) These Clauses apply to the processing of personal data as specified in Annex II.

d) Annexes I to IV are an integral part of the Clauses.

e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2

Invariability of the Clauses

g) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

h) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5 – omitted

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 7

Obligations of the Parties

7.1 Instructions

a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

a) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2 Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3 Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4 Security of processing

a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5 Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6 Documentation and compliance

a) The Parties shall be able to demonstrate compliance with these Clauses.

b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7 Use of sub-processors

a) The processor shall not subcontract any of its processing operations performed on behalf of the controller in accordance with these Clauses to a sub-processor, without the controller's prior specific written authorisation. The processor shall submit the request for specific authorisation at least one month prior to the engagement of the sub- processor in question, together with the information necessary to enable the controller to decide on the authorisation. The list of sub-processors authorised by the controller can be found in Annex IV. The Parties shall keep Annex IV up to date.

b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

c) At the controller's request, the processor shall provide a copy of such a sub- processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub- processor contract and to instruct the sub-processor to erase or return the personal data.

7.8 International transfers

a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub- processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8

Assistance to the controller

a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

   1. the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;
   2. the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;
   3. the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

4. the obligations in Article 32 Regulation (EU) 2016/679/.

d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9

Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679 or under Articles 34 and 35 Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

b) in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679/, shall be stated in the controller's notification, and must at least include:

1. the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
2. the likely consequences of the personal data breach;
3. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

c) in complying, pursuant to Article 34 Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

b) the details of a contact point where more information concerning the personal data breach can be obtained;

c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III – FINAL PROVISIONS

Clause 10

Non-compliance with the Clauses and termination

a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

   1. the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;
   2. the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;
   3. the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

----

place, date controller

----

place, date processor

ANNEX I CONTACT DETAILS OF THE PROCESSOR

Company: EventMobi GmbH

Address: Kopernikusstraße 35, 10243 Berlin, Deutschland

Name, position and contact details of the contact person:

Thorben Grosser (Data Protection Coordinator)

Tel: 030 5557 343 10

Email Address: tg@eventmobi.com

Name and contact details of the Data Protection Officer

Kemal Webersohn (WS-Datenschutz GmbH)

Address: Dircksenstraße 51, 10178 Berlin GERMANY

Phone: 030 88 72 07 88

Email Address: eventmobi@ws-datenschutz.de

ANNEX II: DESCRIPTION OF THE PROCESSING

Categories of data subjects whose personal data is processed

- Customers inside your company
- Participants

Categories of personal data processed

- Address
- Occupation
- E-mail address
- Landline number
- Mobile number
- Name, first name, title
- Optional data defined by the organizer

Nature of the processing

- The Processor provides a platform for collecting, storing and organizing the personal data of the Participants.

Purpose(s) for which the personal data is processed on behalf of the controller

- The object of the processing is the management of the event of the customers designed as a service. This can take place virtually or in person. The Processor offers a complete platform solution for the management of events by means of its own software and the possibility of integrating third-party providers. This begins with the registration of participants, includes the implementation and production of the event, as well as satisfaction surveys and gamifications following the event.

Duration of the processing

- The contractual relationship begins with the signing of this contract and the start of the use of the platform of EventMobi. The contract ends only with the termination of the processing of the personal data of the Controller by the Processor and applies to all events that the Processor manages for the Controller.

ANNEX III TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

1. Admission control

Purpose: To prevent unauthorized persons from gaining access to data processing equipment with which personal data is processed or used.

Measures:

- Access for authorized employees only
- Key protection of the individual office rooms
- Documented key allocation
- Withdrawal of access means after expiration of the authorization

2. Control of Access Rights

Purpose: To prevent data processing systems from being used by unauthorized persons.

Measures:

- Password Policy
- Clean Desk Policy requires each employee to properly dispose of documents and lock computers when leaving the workplace.
- Encryption of data carriers
- Firewall/virus scanner/interface protection
- Organizational instruction for issuing keys
- Immediate blocking of authorizations when employees leave the company
- After creating backups, they are encrypted.
- Backup concept is implemented
- Technical or organizational measures ensure that authorizations that are no longer required are revoked promptly.

3. Access control

Purpose: to ensure that hose authorized to use a data processing system can access only a certain part of the system according to their access authorization and that personal data cannot be read, copied, modified or removed without authorization during processing, use and storage.

Measures:

- Differentiated authorizations (e.g. in the form of profiles, roles)
- Binding authorization allocation procedure
- There is an administration concept for the comprehensible application and allocation of access rights.
- Binding procedure for restoring data from backup
- Allocation of minimal authorizations (need-to-know principle)

4. Separation control

Purpose: To ensure that data collected for different purposes can be processed separately.

Measures:

- Content separation of productive and test environment
- Physical separation (systems, databases, data carriers)
- Multi-client capability of relevant applications
- Control via authorization concept
- Setting database rights
- Data sets are provided with purpose attributes

5. Transfer control

Purpose: to ensure that personal data cannot be read, copied, altered, or removed without authorization during electronic transmission or while being transported or stored on data media, and that it is possible to verify and determine to which entities personal data is intended to be transmitted by data transmission equipment.

Measures:

- Secured transport protocols (SSL, TLS, SFTP)
- The ban on the use of private data carriers at the workplace applies
- Work instructions for the use of mobile data carriers
- Procedure for data protection-compliant deletion/disposal of data carriers and documents

6. Input control

Purpose: to ensure that it is possible to check and establish retrospectively whether and by whom personal data has been entered into data processing systems, modified or removed.

Measures:

- Registration of users and time of the respective change in the system
- The organizational definition of responsibilities for those authorized to enter data is documented.
- Each employee has only the necessary access to the data required within the scope of his function/role (principle of minimal rights).
- Authorizations for resources requiring protection are requested and granted only by persons authorized to do so.
- For all users who use personal data, a history is kept that records which user performed which action and when, provided that this action modifies personal data.

7. Control of data processing on behalf

Purpose: To ensure that personal data processed on behalf of the client can only be processed in accordance with the client's instructions.

Measures:

- Control of the execution of the contract
- The contract contains detailed information about the purpose limitation of the client's personal data as well as a prohibition of use by the service provider outside of the written order.
- The contract contains detailed information about the type and scope of the data processing on behalf of the client and use of personal data of the client.
- The service provider has appointed a data protection officer and ensures through the data protection organization that he or she is appropriately and effectively integrated into the relevant operational processes.
- Contracts for data processing on behalf are in place with all relevant subcontractors.
- The clear contract, offer and order confirmation are available.
- The order has been placed in a formalized manner (order form).
- A general safety concept is available.
- All employees authorized to access data are demonstrably bound to data secrecy.
- Every employee has received work instructions/guidelines or fact sheets that provide information on measures for compliance with data protection as well as IT security.
- In the event of errors regarding data processing or violation of data protection, information shall be provided to the Client without delay.

8. Availability control

Purpose: To ensure that personal data is protected against accidental destruction or loss.

Measures:

- Backup procedures/regular backups
- Mirroring hard disks
- Use of protection programs (virus protection, firewall, SPAM filter)
- Automated standard routines for regular updates of protection software (e.g., virus scanners, malware protection, and firewall systems)
- Redundant sites

9. Organizational control

Purpose: To design the in-house organization in such a way that it meets the special requirements of data protection. What is meant by this is that data protection should not adapt to the organization, but the organization should adapt to data protection.

Measures:

- All employees have been obligated in writing to maintain data secrecy and have been instructed accordingly.
- All employees receive regular training (at least once a year) on data protection in the workplace.
- Auditing by the data protection officer(s) is carried out on a regular basis.
- There are defined proxy arrangements within functional groups.
- There is a procedure for regular review, assessment and evaluation (Art. 32 (1) (d) GDPR) in the form of a data protection management system.

10. Privacy by design/Privacy by default etting

Purpose: Privacy by design/Privacy by default

- No more personal data is collected than is necessary for the respective purpose.
- Simple exercise of the right of withdrawal of the data subject by technical measures.

Certified
Data Privacy
Webersohn
& Scholtz
2022

ANNEX IV: LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

Company	***Address***	***Function***
5TouchSolutions, Inc.	207 Queens Quay West, Suite 320, Toronto, ON M5J 1A7 Kanada	Provision, maintenance and servicing of the EventMobi software