doo

Data Processing Agreement

How this Data Processing Agreement is concluded:

This Data Processing Agreement ("DPA") was already signed by doo GmbH. To conclude this DPA, please fill in the field "Customer" and sign on page 3. Then please send the complete DPA back to datenschutz@doo.net.

Upon receipt by us of the unmodified, completed and countersigned DPA, the DPA shall become valid and binding. This DPA is part of the service agreement on the provision of the doo Event Management Platform to the Customer. This DPA is only valid and binding if there is a service agreement between the parties, otherwise it is invalid.

Customer:	
Contractor:	doo GmbH, Hultschiner Straße 8, 81677 Munich, Germany

1. General

(1) The Contractor is the provider of an event management platform as Software as a Service ("Software"). The parties have concluded a contract for the provision of the event management platform together with supplementary services ("Service Agreement"). The performance of the services of the Contractor according to the service agreement also includes the processing of personal data on behalf of the Customer.

(2) This DPA specifies, as part of the Service Agreement, the obligations of both parties to comply with the applicable data protection law, in particular the requirements of the General Data Protection Regulation (GDPR).

2. Scope of Application

The Contractor shall process personal data on behalf of the Customer. The parties agree that for the purposes of this DPA the Customer shall be the Controller and the Contractor shall be the Processor ("Controller" and "Processor" shall have the meaning as defined by the GDPR). The subject-matter of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects are specified in the Service Agreement and in **Annex 1** to this DPA. The term of this DPA depends on the term of the Service Agreement.

3. Compliance with Instructions

(1) The Contractor may only process personal data within the scope of the order and the documented instructions of the Customer. The instructions shall initially be specified in the Service Agreement and may then be changed, supplemented or replaced by the Customer in text form. Verbal instructions are to be confirmed by the Customer immediately in text form.

(2) If the Contractor is obliged to process personal data in accordance with the law of the Union or the Member State to which the Contractor is subject, the Contractor shall inform the Customer thereof in writing prior to the respective processing, unless the law prohibits such information for important reasons of public interest. In the latter case, the Contractor shall inform the Customer immediately as soon as this is legally possible.

(3) The Contractor shall inform the Customer without delay if it is of the opinion that an instruction violates applicable laws. The Contractor may suspend the implementation of the instruction until it has been confirmed or amended by the Customer.

(4) The Contractor may use data concerning the use of the software by the Customer in anonymized form for the purposes of optimizing the software, user experience and for security-relevant evaluations. The Customer hereby issues a corresponding instruction for the corresponding anonymization.

4. Technical and Organisational Measures

(1) The Contractor undertakes towards the Customer to comply with the technical and organisational measures required to comply with the applicable data protection regulations. This includes in particular the provisions of Art. 32 GDPR.

(2) The status of the technical and organisational measures existing at the time of conclusion of this DPA is documented in **Annex 2** to this DPA. The parties agree that changes to the technical and organisational measures may be necessary in order to adapt to technical and legal circumstances. The Contractor reserves the right to change the security measures taken, but it must be ensured that they do not fall below the contractually agreed level of protection. The Customer may at any time request an up-to-date overview of the technical and organisational measures taken by the Contractor.

5. Data Subject Rights

(1) The Contractor shall, taking into account the nature of the processing, assist the Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III (in particular access, correction, blocking or deletion). To the extent that the assistance of the Contractor is necessary for the protection of rights of data subjects by the Customer, the Contractor shall take the necessary measures according to the instructions of the Customer.

(2) The Contractor may only provide information to third parties or to data subjects with the prior consent of the Customer. It shall forward requests addressed directly to the Contractor to the Customer without undue delay.

6. Other Obligations of the Contractor

(1) The Contractor shall inform the customer immediately, at the latest within 48 hours, if it becomes aware of violations of the protection of personal data processed on behalf of the Customer.

(2) The Contractor shall support the Customer in preparing and updating the records of processing activities with regard to the data processing performed by the Contractor on behalf of the Customer, and, if necessary, in carrying out a data protection impact assessment. All necessary information and documentation must be made available to the Customer immediately upon request.

(3) If the Customer is subject to inspection by a supervisory authority or if data subjects assert rights against the Contractor, the Contractor undertakes to support the Customer to the necessary extent insofar as the personal data processed on behalf of the Customer is affected.

(4) The persons employed by the Contractor for the processing have committed themselves in writing to confidentiality, have been made familiar with the relevant provisions of all relevant data protection laws and are continuously appropriately instructed and monitored with regard to the fulfilment of data protection requirements.

(5) The Contractor shall support the Customer in complying with the obligations set out in Articles 32 to 36 GDPR, taking into account the type of processing and the information available to the Contractor.

(6) The Contractor has appointed a competent and reliable person as data protection officer. The Customer may contact the data protection officer directly (datenschutz@doo.net) for any questions with regard to data processing.

7. Rights and Obligations of the Customer

(1) The Customer shall be responsible for assessing the lawfulness of the data processing and for safeguarding the rights of data subjects.

(2) The Customer shall be entitled to monitor and audit compliance with the provisions on data protection and the contractual agreements at the Contractor to a reasonable extent itself or by third parties, in particular by obtaining information and inspecting the stored data and data processing programs. The Contractor shall, as far as necessary and possible, provide access and insight to the persons entrusted with the inspection. The Contractor is obliged to provide necessary information, to demonstrate procedures and to provide evidence which is necessary for the performance of an inspection. Inspections at the Contractor's premises shall be carried out without avoidable disruptions to its business operations. Unless otherwise indicated for urgent reasons to be documented by the Customer, inspections shall take place after reasonable advance notice and during business hours of the Contractor and not more frequently than every 12 months.

8. Subprocessors

(1) The Contractor may only use subprocessors with the consent of the Customer. The Customer consents to the usage of subprocessors according to doo's List of Subprocessors, accessible at https://doo.net/de/about/rechtliches/downloads.html. doo's List of Subprocessors also defines the process for future changes of subprocessors.

(2) The Contractor must carefully select its subprocessors and check before using them that they can comply with the agreements made between the Customer and the Contractor. In particular, the Contractor shall check that all subcontractors have taken the necessary technical and organisational measures to protect personal data in accordance with Art. 32 GDPR.

(3) Services which the Contractor uses with third parties as a pure ancillary service in order to carry out its business activities shall not be considered subproceessing in the context of this DPA. This includes, for example, cleaning services, pure telecommunications services without concrete reference to services provided by the Contractor for the Customer, postal and courier services, transport services and security services.

(4) The usage of subprocessors shall not affect the Contractor's contractual and data protection obligations towards the Customer. The Contractor shall be liable for any acts or omissions of its subprocessors as if they were its own acts or ommissions.

9. Data Transfer to Third Countries

Data is also processed by the Contractor in third countries (outside of the EEA). The transfer of personal data to a third country by the Contractor is carried out on the basis of an adequacy decision in accordance with Art. 45 GDPR and/or on the basis of suitable guarantees in accordance with Art. 46 GDPR (e.g. Standard Contract Clauses/Standard Data Protection Clauses issued by the Commission and concluded between the Contractor and the subprocessor in a third country).

10. Deletion and Return of Personal Data

(1) Copies of the personal data processed on behalf of the Customer shall not be made without the knowledge of the Customer. Excluded from this are backup copies insofar as they are necessary to guarantee proper data processing, as well as data which are necessary with regard to compliance with statutory retention obligations.

(2) Upon termination of the Service Agreement or earlier upon request by the Customer, the Contractor shall hand over the data to the Customer or delete such data in accordance with the requirements of applicable data protection laws nd regulations.

(3) Documentations which serve as proof of the orderly and proper data processing shall be stored by the Contractor beyond the end of the contract in accordance with the respective retention periods.

Customer
Name and Function/Title:
Date:
Signature:

Contractor
Name and Function/Title:
Christoph Sedlmeir, Managing Director
Date:
February 5, 2021
Signature:
DocuSigned by: Christoph Sedlmeir A8B52D7251A34BD...

Annex 1: Description of the Data Processing

Controller

The Customer named above is the controller and uses the Contractor's event management platform.

Processor

The Contractor provides its event management platform to the Customer as Software as a Service (SaaS).

Types of Personal Data

The personal data processed concern the following data subjects and types of personal data:

- Data of contacts transferred by the Customer to the event management platform to be invited to an event ("Invitee Data")
- Participants in events that have either registered directly for an event via the event management platform or have been transferred to the event management platform by the Customer as participants ("Attendee Data")

Categories of Data

The personal data processed belong to the following categories of data:

- Name
- Address
- Email address
- Transaction data at events ("session tracking")
- Payment data (for chargeable events)
- Reaction behaviour (Invitee Data)
- Other data transferred to the event management platform by the Customer or requested by the Customer as part of an event registration process

Special Categoris of Data

The personal data processed on behalf of the Customer usually does not include any special categories of data, unless the Customer transfers special categories of data to the event management platform or requests them as part of the registration for an event.

Subject-matter and Duration of Processing

The personal data processed is processed for the organization and management of events, including invitation/marketing, registration, billing, participation. The duration of the processing corresponds, subject to Section 10 of this DPA, to the duration of the Service Agreement.

Annex 2: Technical and Organizational Measures

doo implemented the following technical and organizational data security measures within the meaning of Art. 32 GDPR with regard to the doo event management platform:

1. CONFIDENTIALITY

1.1 Physical Access Control

The hosting of the servers is provided by Amazon Web Services (AWS) in Frankfurt am Main. Access is ensured by a separation system. Furthermore, the entire site outside and inside the data centers is protected by video surveillance and 365x7x24 security personnel.

Details: https://aws.amazon.com/de/compliance/data-center/controls/

1.2 System Access Control

As far as servers are concerned, sufficient certified technical personnel is available on site during the day. Outside the guaranteed times, the travel time for the personnel mentioned in sentence 1 is less than one hour.

With regard to doo's personnel, access to the administration tools is ensured as follows:

- Access is secured by a password with minimum length.
- Access for employees is ensured via ACLs (Access Control Lists)
- Organizational measures in case employees leave the company (deletion of access)

With regard to the Organizer's user account, access is guaranteed as follows:

- The access is secured by a password with minimum length
- Access is exclusively via an SSL-encrypted connection.

1.3 Data Access Control

Demand-oriented design of the authorization concept and the access rights ("need to know") as well as their monitoring and logging.

With doo, access control is guaranteed via ACLs (Access Control Lists) which only allow employees access to the areas they need for their work (Principle of least privilege). Furthermore, there are organizational measures in case employees leave the company (deletion of access).

1.4 Separation

The doo systems are used by several clients simultaneously (multitenancy) and guarantee a logical separation of the data of the customers. At the same time there is a physical separation of the systems according to function in development system, test system and productive system.

1.5 Encryption

Administrative access to server systems is always via encrypted connections. In addition, data on server and client systems is stored on encrypted data carriers. Corresponding hard disk encryption systems are in use.

2. INTEGRITY

2.1 Input Control

Personal data can be assigned to its origin at any time. doo undertakes all necessary steps to be able to authenticate the originators of the data correctly (in particular in connection with electronic payment transactions).

Only three groups are authorized to enter data into the system, in each of which the origin is documented and assignable:

- Ticket purchasers: deposit email address and further information. Registration can only be guaranteed if the email address is functioning. doo also generates a corresponding timestamp. Ticket purchases and user interactions are logged by doo.
- Organiser: Authentication takes place via user-specific passwords. Access without authentication is not possible. Every Organiser login into the system is automatically logged by doo.
- Customer service/IT: Authenticate via user-specific passwords. Access without authentication is not possible.

2.2 Transfer Control

If personal data must be exchanged, this happens within the systems of doo or its subprocessors. The data thus lies on the systems and does not leave the network to which all systems are connected. This also ensures that only persons who have access to the machines can obtain this data. All connections between the systems are either local or SSL encrypted.

Personal data is not changed in the course of transmission and processing and remains intact, complete and up-to-date. The Contractor shall do everything necessary to prevent data from being falsified or incorrect data from being processed. At the same time, it is guaranteed that changes to data can be traced.

The technical service provider of doo is certified according to ISO 27001, so that through backup systems and similar mechanisms the probability of an integrity endangering data decoherence is very low.

3. AVAILABILITY AND RESILIENCE

Data on doo's server systems are regularly backed up comprehensively according to a detailed backup policy. The import of backups is tested regularly.

The IT systems have an uninterruptible power supply. The server room is equipped with a fire alarm system and a CO2 extinguishing system. All server systems are subject to monitoring, which immediately triggers messages to an administrator in case of malfunctions.

There is also an emergency plan at doo, which includes a restart plan.

In addition, the measures implemented with regard to the servers at the technical service provider AWS are documented in detail here: https://aws.amazon.com/de/security/

4. ORDER CONTROL

Within the scope of order control, doo ensures that the data to be processed in the order will only be processed in accordance with the instructions given in the service description.

The procedures for the processing of personal data are completely and up-to-date documented, so that these can be traced by the Customer in a reasonable amount of time.

Persons entitled to issue instructions to the Contractor are the management and the data protection officer of the Customer.

Hosting of the servers is provided by AWS. There are contracts between doo and AWS.

5. PRIVACY BY DESIGN AND PRIVACY BY DEFAULT

doo takes care to ensure that the principle of necessity is taken into account in the context of user interfaces already during the development of the software. For example, form fields can be designed flexibly and mandatory fields can be provided or fields can be deactivated.

doo's software supports input control by a flexible and customizable audit trail, which allows an unchangeable storage of changes to data and user permissions. Permissions on data or applications can be set flexibly and granularly.

6. PROCEDURES FOR REGULAR REVIEW, ASSESSMENT AND EVALUATION

At doo, a data protection management system has been implemented and a data protection officer has been designated.

There is a policy on data protection and information security and guidelines to ensure the implementation of the policy's objectives. The policy and guidelines are regularly evaluated and adjusted with regard to their effectiveness.

A data protection and information security team has been set up to plan, implement, evaluate and make adjustments to data protection and information security measures.

All employees receive regular training in data protection and information security. In particular, it is ensured that data breaches and security incidents are recognized by all employees and reported immediately to the data protection and information security team. The data protection and information security team will investigate the incident immediately. If data processed on behalf of customers is affected, care is taken to ensure that they are informed immediately about the nature and scope of the incident.