DATA PROCESSING ADDENDUM

pursuant to the EU standard contractual clauses from Commission Implementing Decision 2021/915 of June 4, 2021

Where is the template for this Data Processing Addendum coming from?

This Data Processing Addendum (pursuant to Implementing Decision 2021/915) is the EU Commission's standard contractual clauses for processing operations within the EU and is therefore a quasi-model contract for processing agreements pursuant to Art. 28 GDPR.

It is NOT the standard contractual clauses for the transfer of personal data to third countries (pursuant to Implementing Decision 2021/914).

In our opinion, if the EU Commission provides a model contract, it is a good idea to use it as well, since the use of the model contract gives both parties the security of concluding a contract processing agreement that meets the requirements of Art. 28 GDPR without having to examine an individual contract in detail.

The EU standard contractual clauses are used below unchanged as specified by the EU Commission. The music plays in the annexes I to IV:

Annex I: ***List of Parties***
Annex II: ***Description of the Processing***
Annex III: ***Technical and Organizational Measures***
Annex IV: ***List of Sub-processors***

How is this Data Processing Addendum concluded?

This Data Processing Addendum has already been signed by the Processor (on page 7 below).

To conclude this Data Processing Addendum, please fill in the "Controller" details on page 7 below. Then please sign this Data Processing Addendum on page 7 below.

Then please send the Data Processing Addendum back to **datenschutz@doo.net**.

The Addendum shall become valid upon receipt by us of the unmodified, completed and countersigned Addendum. This Data Processing

Addendum is part of the main contract between the parties on the use of the doo event management platform. This Data Processing Addendum is only effective if such a main contract exists between the parties, otherwise it is invalid.

DATA PROCESSING ADDENDUM

pursuant to the EU standard contractual clauses from Commission Implementing Decision 2021/915 of June 4, 2021

SECTION I

Clause 1: Purpose and scope

a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Art. 28(3) and (4) GDPR.

b) The controllers and processors listed in **Annex I** have agreed to these Clauses in order to ensure compliance with Art. 28(3) and (4) GDPR.

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 GDPR.

f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of GDPR.

Clause 2: Invariability of the Clauses

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

b) 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: Docking clause

a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

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.

Clause7: 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.

b) 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

The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 14 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

a) 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.

b) 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.

c) 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.

d) 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 Art. 32 GDPR.

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 Art. 33 and 34 GDPR, 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 Art. 33 (3) GDPR, 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.

c) 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.

d) in complying, pursuant to Article 34 GRPR, 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 Art. 33 and 34 GDPR.

SECTION III: FINAL PROVISIONS

Clause 10: Non-compliance with the Clauses and termination

a) Without prejudice to any provisions of GDPR, 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 GDPR;

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 GDPR.

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.

ANNEX I:
LIST OF PARTIES

Controller	
Name:	
Address:	
Contact person's name, position and contact details:	
Name and contact details of the data protection officer (if any)	
Date and Signature:	

Processor	
Name:	doo GmbH
Address:	Hultschiner Straße 8, 81677 Munich, Germany
Contact person's name, position and contact details:	Christoph Sedlmeir, Managing Director Email: christoph.sedlmeir@doo.net
Name and contact details of the data protection officer (if any)	Christian Schmoll Email: schmoll@lucid-compliance.com
Date and Signature:	June 18, 2024 DocuSigned by: Christoph Sedlmeir A8B52D7251A34BD...

ANNEX II:
DESCRIPTION OF THE PROCESSING

Subject Matter, Type and Purpose of Processing

The Controller uses the data processor's event management platform. The data processor provides the Controller with the event management platform as software as a service (SaaS) to enable the Controller to organise, manage and run events (online, offline and hybrid, including invitations/marketing, registration, billing, participation).

The processor acts as a data processor within the meaning of Art. 28 GDPR for the customer. The customer is the Controller within the meaning of the GDPR and uses the data processor's software to collect and process personal data.

Data Subjects

The personal data processed concern the following categories of data subjects:

- Data transferred to the event management platform by the customer regarding their contacts who are to be invited to an event ("Invitee Data")
- Attendees at events who have either registered for an event directly via the event management platform or who have been transferred to the event management platform as attendees by the customer ("Attendee Data")

Categories of Data

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

- Name
- Address
- Email address
- Movement data at events ("session tracking"), if used
- Payment data (for chargeable events)
- Reaction behaviour (Invitee Data)
- other data transferred by the customer to the event management platform or requested as part of registration for an event

The personal data processed on behalf of the customer does not regularly include any special categories of data, unless special categories of data are transferred to the event management platform by the client or requested as part of a registration for an event.

Duration of the Processing

The data processing is performed by the Processor for the duration of the respective main contract.

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

ISO 27001

With regard to the technical and organisational measures, reference is generally made to the ISO 27001 certification of doo GmbH. The certificate can be found as an appendix to this Annex III.

In addition to the ISO 27001 certification, an overview of the technical and organisational measures is provided below:

Confidentiality

Physical Access Control

The hosting of the servers is provided by AWS in Frankfurt am Main. Access is secured by a singularization 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/

System Access Control

Sufficient certified technical personnel are available on site during the day for the servers. Outside the guaranteed times, the journey time for the personnel mentioned in sentence 1 is less than one hour.

With regard to doo personnel, access to the administration tools is secured as follows:

- Access is secured by a password with a minimum length
- Employee access is secured via ACLs (Access Control Lists)
- Organisational measures if employees leave the company (deletion of access)

Access to the organiser's user account is secured as follows:

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

Data Access Control:

Needs-based design of the authorisation concept and access rights as well as their monitoring and logging.

At doo, data access control is ensured via ACLs (Access Control Lists) which only grant employees access to the areas they need for their work (principle of least privilege). There are also organisational measures in place if employees leave the company (deletion of access).

Separation

The doo systems are used by several clients at the same time (client capability) and guarantee a logical separation of the clients' data. At the same time, there is a physical separation of the systems according to function into development system, test system and productive system.

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. Appropriate hard disk encryption systems are in use.

Integrity

Transfer control:

If personal data has to be exchanged, this takes place within the systems of doo or the sub-processors. The information is therefore stored on the systems and does not leave the network to which all systems are connected. This also ensures that only people who have access to the machines can obtain this data. All connections between the systems are either local or encrypted via SSL.

Personal data is not changed in the course of transfer 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 ensured that changes to data can be traced.

doo's technical service provider is certified in accordance with ISO 27001, so that the probability of data decoherence jeopardising integrity is very low thanks to backup systems and similar mechanisms.

Input control:

Personal data can be assigned to its origin at any time. doo does everything necessary to correctly authenticate the originators of the data (especially in connection with electronic payment transactions).

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

- Ticket purchasers: Enter e-mail address and other information. Registration can only be ensured if the e-mail address is functional. doo also generates a corresponding timestamp. Ticket purchases and user interactions are logged by doo.
- Organiser: Authentication takes place via user-specific passwords. Entry without authentication is not possible. Every organiser login to the system is automatically logged by doo.
- Customer service/IT: Authentication via user-specific passwords. Entry without authentication is not possible.

Availability and Resilience

Data on doo server systems is regularly and comprehensively backed up in accordance with a detailed backup policy. The import of backups is tested regularly.

The IT systems have an uninterruptible power supply. There is a fire alarm system and a CO2 extinguishing system in the server room. All server systems are subject to monitoring, which immediately triggers notifications to an administrator in the event of faults.

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

The measures implemented by the technical service provider AWS with regard to the servers are also documented in detail here: https://aws.amazon.com/de/security/

Privacy by Design und Privacy by Default

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

doo's software supports input control with a flexible and customisable audit trail that enables unalterable storage of changes to data and user authorisations. Authorisations for data or applications can be set flexibly and granularly.

Procedures for Periodic Review and Evaluation

Data protection management:

- Complete and up-to-date documentation of procedures and processing directory
- Appointment of an experienced and expert Data Protection Officer

- All employees are obliged to data protection and confidentiality
- Regular data protection trainings for all employees
- Annual audits by the Data Protection Officer

Incident response management:

- Any incidents are reported immediately to the Information Security Officer and the Data Protection Officer
- Processing of any cases jointly by the Information Security Officer and the Data Protection Officer

Order control:

- Written data processing agreements are concluded with all customers
- Ensuring the deletion of data after completion of the order
- Effective control rights agreed with the Contractor

Appendix to Annex III: ISO Certificate

ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

TÜV SÜD Management Service

CERTIFICATE

Certificate Registration No.: **12 310 67685 TMS** / Order No.: **707173958**

The Certification Body
of TÜV SÜD Management Service GmbH

certifies that the organization

doo GmbH
Hultschiner Str. 8
81677 München
Germany

for the scope

Development, provisioning and operation
of event management solutions

has established and applies an Information Security Management System according to "Statement of Applicability".

An audit was performed and has furnished proof that the requirements according to

ISO/IEC 27001:2022

are fulfilled.

The certificate is valid from **2024-06-05** until **2027-06-04**.

Version of the statement of applicability: **1.0 vom 24.Jan. 2024**

Fred Wenke
Head of Certification Body
Munich, 2024-06-05

IAF DAkkS Deutsche Akkreditierungsstelle D-ZM-14143-01-00

MS/01-07/2023

TÜV SÜD Management Service GmbH • Zertifizierungsstelle • Ridlerstrasse 57 • 80339 München • Germany
www.tuvsud.com/de-certificate-validity-check

TÜV®

ANNEX IV:
LIST OF SUB-PROCESSORS

The List of Sub-processors is available at https://www.doo.net/download.