ERGÄNZUNGSVEREINBARUNG AUFTRAGSVERARBEITUNG

gemäß der EU-Standardvertragsklauseln aus dem Durchführungsbeschluss 2021/915 der Kommission vom 4. Juni 2021

Woher stammt die Vorlage für diese Ergänzungsvereinbarung Auftragsverarbeitung?

Es handelt sich bei dieser Ergänzungsvereinbarung Auftragsverarbeitung (gemäß Durchführungsbeschluss 2021/915) um die Standardvertragsklauseln der EU-Kommission für Auftragsverarbeitungen innerhalb der EU und damit quasi um einen Mustervertrag für Auftragsverarbeitungsvereinbarungen gemäß Art. 28 DSGVO.

Es handelt sich NICHT um die Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer (gemäß Durchführungsbeschluss 2021/914).

Wenn die EU-Kommission einen Mustervertrag zur Verfügung stellt, bietet es sich unseres Erachtens an, diesen auch zu verwenden, da die Verwendung des Mustervertrages beiden Parteien die Sicherheit gibt, eine Auftragsverarbeitungsvereinbarung abzuschließen, die den Anforderungen des Art. 28 DSGVO genügt, ohne einen Individualvertrag im Detail prüfen zu müssen.

Die EU-Standardvertragsklauseln werden nachfolgend unverändert wie von der EU-Kommission vorgegeben verwendet. Die Musik spielt in den Anhängen I bis IV:

Anhang I: ***Liste der Parteien***
Anhang II: ***Beschreibung der Verarbeitung***
Anhang III: ***Technische und organisatorische Maßnahmen***
Anhang IV: ***Liste der Unterauftragsverarbeiter***

Wie wird diese Ergänzungsvereinbarung Auftragsverarbeitung abgeschlossen?

Diese Ergänzungsvereinbarung Auftragsverarbeitung regelt die Datenverarbeitung durch die doo GmbH als Auftragsverarbeiter im Auftrag des Kunden im Rahmen der Nutzung der Event-Management-Plattform von doo.

Sie ist Bestandteil des Vertrages über die Nutzung der Event-Management-Plattform von doo durch den im jeweiligen Auftrag/Vertrag genannten Kunden. Sie wird durch Bezugnahme in den AGB Bestandteil des jeweiligen Vertrages.

Alternativ ist eine vorunterzeichnete Version dieses Datenverarbeitungszusatzes abrufbar unter https://www.doo.net/download.

ERGÄNZUNGSVEREINBARUNG AUFTRAGSVERARBEITUNG

gemäß der EU-Standardvertragsklauseln aus dem Durchführungsbeschluss 2021/915 der Kommission vom 4. Juni 2021

ABSCHNITT I

Klausel 1: Zweck und Anwendungsbereich

a) Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) soll die Einhaltung von Art. 28 Abs. 3 und 4 DSGVO sichergestellt werden.

b) Die in **Anhang I** aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Art. 28 Abs. 3 und 4 DSGVO zu gewährleisten.

c) Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß **Anhang II**.

d) Die **Anhänge I bis IV** sind Bestandteil der Klauseln.

e) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der DSGVO unterliegt.

f) Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der DSGVO erfüllt werden

Klausel 2: Unabänderbarkeit der Klauseln

a) Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.

b) Dies hindert die Parteien nicht daran die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

Klausel 3: Auslegung

a) Werden in diesen Klauseln die in der DSGVO definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.

b) Diese Klauseln sind im Lichte der Bestimmungen der DSGVO auszulegen.

c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der DSGVO vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

Klausel 4: Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

Klausel 5: Kopplungsklausel

a) Eine Einrichtung, die nicht Partei dieser Klauseln ist, kann diesen Klauseln mit Zustimmung aller Parteien jederzeit als Verantwortlicher oder als Auftragsverarbeiter beitreten, indem sie die Anhänge ausfüllt und Anhang I unterzeichnet.

b) Nach Ausfüllen und Unterzeichnen der unter Buchstabe a genannten Anhänge wird die beitretende Einrichtung als Partei dieser Klauseln behandelt und hat die Rechte und Pflichten eines Verantwortlichen oder eines Auftragsverarbeiters entsprechend ihrer Bezeichnung in Anhang I.

c) Für die beitretende Einrichtung gelten für den Zeitraum vor ihrem Beitritt als Partei keine aus diesen Klauseln resultierenden Rechte oder Pflichten.

ABSCHNITT II: PFLICHTEN DER PARTEIEN

Klausel 6: Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in **Anhang II** aufgeführt.

Klausel 7: Pflichten der Parteien

7.1. Weisungen

a) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.

b) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die DSGVO oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

7.2. Zweckbindung

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in **Anhang II** genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

7.3. Dauer der Verarbeitung personenbezogener Daten

Die Daten werden vom Auftragsverarbeiter nur für die in **Anhang II** angegebene Dauer verarbeitet.

7.4. Sicherheit der Verarbeitung

a) Der Auftragsverarbeiter ergreift mindestens die in Anhang III aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.

b) Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7.5. Sensible Daten

Falls die Verarbeitung personenbezogene Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten

zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten“), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

7.6. Dokumentation und Einhaltung der Klauseln

a) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können

b) Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der DSGVO hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.

d) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.

e) Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung

7.7. Einsatz von Unterauftragsverarbeitern

Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens 14 Tage im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

a) Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesen Klauseln und gemäß der DSGVO unterliegt.

b) Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

c) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

d) Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche – im Falle, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben

7.8. Internationale Datenübermittlungen

a) Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 im Einklang stehen.

b) Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 7.7 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der DSGVO beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der DSGVO sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Art. 46 Abs. 2 DSGVO erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

Klausel 8: Unterstützung des Verantwortlichen

a) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.

b) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.

c) Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 8 Buchstabe b zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:

   1) Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung“), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;

   2) Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft

   3) Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;

   4) Verpflichtungen gemäß Art. 32 DSGVO.

d) Die Parteien legen in **Anhang III** die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

Klausel 9: Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Art. 33 und 34 DSGVO nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

9.1. Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

a) bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);

b) bei der Einholung der folgenden Informationen, die gemäß Art. 33 Abs. 3 DSGVO in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:

   1) die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze

   2) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten

   3) die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

c) Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt

d) bei der Einhaltung der Pflicht gemäß Art. 34 DSGVO, die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat

9.2. Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

a) eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);

b) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;

c) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

Die Parteien legen in Anhang III alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Art. 33 und 34 DSGVO zu unterstützen.

ABSCHNITT III: SCHLUSSBESTIMMUNGEN

Klausel 10: Verstöße gegen die Klauseln und Beendigung des Vertrags

a) Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.

b) Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn

   1) der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;

   2) der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der DSGVO nicht erfüllt;

   3) der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln oder der DSGVO zum Gegenstand hat, nicht nachkommt.

c) Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 7.1 Buchstabe b verstoßen.

d) Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

ANHANG I:
LISTE DER PARTEIEN

Verantwortlicher	
Name:	*Im Auftrag/Vertrag bezeichneter Kunde/Auftraggeber*
Anschrift:	*Adresse des Kunden/Auftraggebers wie im Auftrag/Vertrag definiert*
Name, Funktion und Kontaktdaten der Kontaktperson:	*Kontaktperson wie im Auftrag/Vertrag definiert*
ggf. Name und Kontaktdaten des Datenschutzbeauftragten:	*Datenschutzbeauftragter wie im Auftrag/Vertrag definiert*

Auftragsverarbeiter	
Name:	doo GmbH
Anschrift:	Hultschiner Straße 8, 81677 München, Deutschland
Name, Funktion und Kontaktdaten der Kontaktperson:	Christoph Sedlmeir, Geschäftsführer E-Mail: christoph.sedlmeir@doo.net
ggf. Name und Kontaktdaten des Datenschutzbeauftragten:	Christian Schmoll E-Mail: schmoll@lucid-compliance.com

ANHANG II:
BESCHREIBUNG DER VERARBEITUNG

Gegenstand, Art und Zweck der Verarbeitung

Der Verantwortliche nutzt die Event-Management-Plattform des Auftragsverarbeiters. Der Auftragsverarbeiter stellt dem Verantwortlichen die Event-Management-Plattform als Software as a Service (SaaS) zur Verfügung, um ihm die Organisation, das Management und die Durchführung von Events (online, offline und hybrid, einschließlich Einladung/Marketing, Anmeldung, Abrechnung, Teilnahme, zu ermöglichen.

Der Auftragsverarbeiter wird dabei als Auftragsverarbeiter im Sinne des Art. 28 DSGVO für den Auftraggeber tätig. Der Auftraggeber ist Verantwortlicher im Sinne der DSGVO und nutzt die Software des Auftragsverarbeiters zur Erhebung und Verarbeitung personenbezogener Daten.

Betroffene

Die im Auftrag verarbeiteten personenbezogenen Daten betreffen folgende Kategorien Betroffener:

- Vom Auftraggeber in die Event-Management-Plattform transferierte Daten seiner Kontakte, die zu einem Event eingeladen werden sollen („Invitee Data“)
- Teilnehmer an Veranstaltungen, die sich entweder direkt über die Event-Management-Plattform zu einem Event angemeldet haben oder vom Auftraggeber als Teilnehmer in die Event-Management-Plattform transferiert wurden („Attendee Data“)

Datenkategorien

Die im Auftrag verarbeiteten personenbezogenen Daten gehören zu folgenden Datenkategorien:

- Name
- Adresse
- E-Mail-Adresse
- Bewegungsdaten auf Events („Session Tracking“), sofern genutzt
- Zahlungsdaten (bei kostenpflichtigen Events)
- Reaktionsverhalten bei Invitee Data
- Sonstige Daten, die vom Auftraggeber in die Event-Management-Plattform transferiert bzw. im Rahmen einer Anmeldung zu einem Event abgefragt werden

Die im Auftrag verarbeiteten personenbezogenen Daten umfassen regelmäßig keine besonderen Datenkategorien, es sei denn, es werden besondere Datenkategorien vom Auftraggeber in die Event-Management-Plattform transferiert bzw. im Rahmen einer Anmeldung zu einem Event abgefragt.

Dauer der Verarbeitung

Die Datenverarbeitung wird vom Auftragsverarbeiter für die Dauer des jeweiligen Auftrags/Vertrages durchgeführt.

ANHANG III:
TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN

ISO 27001

Hinsichtlich der technischen und organisatorischen Maßnahmen wird grundsätzlich auf die ISO 27001-Zertifizierung der doo GmbH verwiesen. Das Zertifikat findet sich als Anlage zu diesem Anhang III.

In Ergänzung zur ISO 27001-Zertifizierung wird im Folgenden ein Überblick über die technischen und organisatorischen Maßnahmen gegeben:

Vertraulichkeit

Zutrittskontrolle

Das Hosting der Server wird von AWS in Frankfurt am Main bereitgestellt. Der Zugang wird per Vereinzelungsanlage sichergestellt. Weiterhin ist das gesamte Gelände außerhalb und innerhalb der Rechenzentren durch Videoüberwachung und 365x7x24 Sicherheitspersonal geschützt.

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

Zugangskontrolle

Bezüglich der Server ist tagsüber ausreichend zertifiziertes, technisches Personal vor Ort verfügbar. Außerhalb der garantierten Zeiten liegt der Anfahrtsweg für das in Satz 1 genannte Personal unter einer Stunde.

Bezüglich des Personals von doo wird der Zugang zu den Administrationstools sichergestellt wie folgt:

- Zugang ist abgesichert durch ein Passwort mit Mindestlänge
- Zugang der Mitarbeitenden wird über ACLs sichergestellt (Access Control Lists)
- Organisatorische Maßnahmen, falls Mitarbeitende das Unternehmen verlassen (Löschen des Zugangs)

Bezüglich des Nutzerkontos des Veranstalters wird der Zugang wie folgt sichergestellt:

- Der Zugang ist abgesichert durch ein Passwort mit Mindestlänge
- Der Zugang erfolgt ausschließlich über eine SSL-verschlüsselte Verbindung

Zugriffskontrolle:

Bedarfsorientierte Ausgestaltung des Berechtigungskonzeptes und der Zugriffsrechte sowie deren Überwachung und Protokollierung.

Bei doo ist die Zugriffskontrolle über ACLs gewährleistet (Access Control Lists) welche der/dem Mitarbeitenden nur Zugriff auf die Bereiche gewährt die sie/er für die konkrete Tätigkeit benötigt (Principle of least privilege). Weiterhin gibt es organisatorische Maßnahmen, falls Mitarbeitende das Unternehmen verlassen (Löschen des Zugangs).

Trennung

Die Systeme von doo werden von mehreren Mandanten gleichzeitig genutzt (Mandantenfähigkeit) und gewährleisten eine logische Trennung der Daten der Mandanten. Gleichzeitig gibt es eine physikalische Trennung der Systeme nach Funktion in Entwicklungssystem, Testsystem und Produktivsystem.

Verschlüsselung

Ein administrativer Zugriff auf Serversysteme erfolgt grundsätzlich über verschlüsselte Verbindungen. Darüber hinaus werden Daten auf Server- und Clientsystemen auf verschlüsselten Datenträgern gespeichert. Es befinden sich entsprechende Festplattenverschlüsselungssysteme im Einsatz.

Integrität

Weitergabekontrolle:

Wenn personenbezogene Daten ausgetauscht werden müssen, geschieht dies innerhalb der Systeme von doo bzw. der Unterauftragsverarbeiter. Die Informationen liegen somit auf den Systemen und verlassen das Netzwerk, mit dem alle Systeme verbunden sind, nicht. Somit ist auch gewährleistet, dass nur Personen, die Zugriff auf die Maschinen haben, diese Daten erlangen können. Alle Verbindungen zwischen den Systemen erfolgen entweder lokal oder sind über SSL verschlüsselt.

Personenbezogene Daten werden im Zuge der Weitergabe und Verarbeitung nicht verändert und bleiben unversehrt, vollständig und aktuell. doo unternimmt alles Notwendige, um zu verhindern, dass Daten verfälscht werden oder falsche Daten verarbeitet werden. Gleichzeitig ist gewährleistet, dass Änderungen an Daten nachvollzogen werden können.

Der technische Dienstleister von doo (Rechenzentren) ist zertifiziert nach ISO 27001, so dass durch Backup-Systeme und ähnliche Mechanismen die Wahrscheinlichkeit für eine integritätsgefährdende Datendekoherenz sehr gering ist.

Eingabekontrolle:

Personenbezogene Daten können jederzeit ihrem Ursprung zugeordnet werden. doo übernimmt alles Notwendige, um die Urheber der Daten korrekt authentifizieren zu können (insbesondere im Zusammenhang mit dem elektronischen Zahlungsverkehr).

Eingabeberechtigt, um Daten in das System zu schreiben sind nur drei Gruppen, bei denen jeweils der Ursprung dokumentiert und zuordenbar ist:

- Ticketkäufer: Hinterlegen E-Mail-Adresse und weitere Informationen. Nur bei funktionierender E-Mail-Adresse kann Anmeldung sichergestellt werden. doo erzeugt zusätzlich einen entsprechenden Timestamp. Ticketkäufe und Nutzerinteraktionen werden von doo geloggt.
- Veranstalter: Authentifizieren erfolgt über nutzerspezifische Passwörter. Eine Eingabe ohne Authentifizierung ist nicht möglich. Jeder Veranstalter Login in das System wird von doo automatisch geloggt.
- Kundenservice/IT: Authentifizieren sich über nutzerspezifische Passwörter. Eine Eingabe ohne Authentifizierung ist nicht möglich.

Verfügbarkeit und Belastbarkeit

Daten auf Serversystemen von doo werden entsprechend einer detaillierten Backup-Policy regelmäßig umfassend gesichert. Das Einspielen von Backups wird regelmäßig getestet.

Die IT-Systeme verfügen über eine unterbrechungsfreie Stromversorgung. Im Serverraum befindet sich eine Brandmeldeanlage sowie eine CO2-Löschanlage. Alle Serversysteme unterliegen einem Monitoring, das im Falle von Störungen unverzüglich Meldungen an einen Administrator auslöst.

Es gibt bei doo zudem einen Notfallplan, der auch einen Wiederanlaufplan beinhaltet.

Zudem sind die bezüglich der Server beim technischen Dienstleister AWS umgesetzten Maßnahmen hier im Detail dokumentiert: https://aws.amazon.com/de/security/

Privacy by Design und Privacy by Default

Bei doo wird schon bei der Entwicklung der Software Sorge dafür getragen, dass dem Grundsatz der Erforderlichkeit schon im Zusammenhang mit Benutzer-Interfaces Rechnung getragen wird. So sind z.B. Formularfelder flexibel gestaltbar und es können Pflichtfelder vorgesehen oder Felder deaktiviert werden.

Die Software von doo unterstützt die Eingabekontrolle durch einen flexiblen und anpassbaren Audit-Trail, der eine unveränderliche Speicherung von Änderungen an Daten und Nutzerberechtigungen ermöglicht. Berechtigungen auf Daten oder Applikationen können flexibel und granular gesetzt werden.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung
Datenschutzmanagement: • Vollständige und aktuelle Dokumentation von Verfahren und Verarbeitungsverzeichnis • Benennung eines erfahrenen und fachkundigen Datenschutzbeauftragten • Einhaltung Datengeheimnis, sämtliche Mitarbeitenden sind auf Datenschutz und Vertraulichkeit verpflichtet • Regelmäßige Datenschutzschulungen für alle Mitarbeitenden • jährliche Audits durch den Datenschutzbeauftragten **Incident-Response-Management:** • Etwaige Vorfälle werden unverzüglich dem Informationssicherheitsbeauftragten und dem Datenschutzbeauftragten gemeldet • Bearbeitung etwaiger Fälle gemeinsam durch den Informationssicherheitsbeauftragten und den Datenschutzbeauftragten **Auftragskontrolle:** • Schriftliche Verträge zur Auftragsverarbeitung werden mit allen Kunden abgeschlossen • Sicherstellung der Löschung von Daten nach Beendigung des Auftrags • Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart

Anlage zu Anhang III: ISO-Zertifikat

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

TÜV SÜD Management Service

ZERTIFIKAT

Zertifikat-Registrier-Nr.: **12 310 67685 TMS** / Auftrags-Nr.: **707173958**

Die Zertifizierungsstelle
der TÜV SÜD Management Service GmbH

bescheinigt, dass die Organisation

doo

doo GmbH
Hultschiner Str. 8
81677 München
Deutschland

für den Geltungsbereich

Entwicklung, Bereitstellung und Betrieb
von Event-Management-Lösungen

ein Informationssicherheitsmanagementsystem gemäß
„Erklärung zur Anwendbarkeit" eingeführt hat und anwendet.

Durch ein Audit wurde der Nachweis erbracht,
dass die Forderungen der

ISO/IEC 27001:2022

erfüllt sind.

Dieses Zertifikat ist gültig vom **05.06.2024** bis **04.06.2027**.

Version der Erklärung zur Anwendbarkeit: **1.0 vom 24.Jan. 2024**

Fred Wenke
Leiter der Zertifizierungsstelle
München, 05.06.2024

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

VS/01.07/2023

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

TÜV®

ANHANG IV:
LISTE DER UNTERAUFTRAGSVERARBEITER

Die Übersicht der Unterauftragsverarbeiter ist abrufbar unter https://www.doo.net/download.