Vereinbarung Auftragsverarbeitung

Diese Vereinbarung Auftragsverarbeitung regelt die Datenverarbeitung im Auftrag des Auftraggebers durch die doo GmbH als Auftragnehmerin. Sie ist Teil der Leistungsvereinbarung über die Zurverfügungstellung der doo Event-Management-Plattform an den im jeweiligen Auftrag genannten Auftraggeber. Sie wird durch Bezugnahme in den AGB Bestandteil des jeweiligen Vertrages.

1. Allgemeines

(1) Die Auftragnehmerin ist Anbieter einer Event-Management-Plattform als Software as a Service („Software"). Die Parteien haben einen Vertrag über die Zurverfügungstellung der Event-Management-Plattform nebst ergänzender Leistungen abgeschlossen („Leistungsvereinbarung"). Die Erbringung der Leistungen des Auftragnehmers nach der Leistungsvereinbarung umfasst auch die Verarbeitung personenbezogener Daten im Auftrag des Auftraggebers.

(2) Diese Vereinbarung Auftragsverarbeitung („AVV") konkretisiert, als Teil der Leistungsvereinbarung, die Verpflichtungen beider Parteien zur Einhaltung des anwendbaren Datenschutzrechts, insbesondere der Anforderungen der EU Datenschutz-Grundverordnung („DSGVO").

2. Anwendungsbereich

Die Auftragnehmerin verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind in der Leistungsvereinbarung und in **Anlage 1 zu dieser AVV** festgelegt. Die Laufzeit dieser AVV richtet sich nach der Laufzeit der Leistungsvereinbarung.

3. Weisungsgebundenheit

(1) Die Auftragnehmerin darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der dokumentierten Weisungen des Auftraggebers verarbeiten. Die Weisungen werden anfänglich durch die Leistungsvereinbarung festgelegt und können vom Auftraggeber danach in Textform geändert, ergänzt oder ersetzt werden. Mündliche Weisungen sind vom Auftraggeber unverzüglich in Textform zu bestätigen.

(2) Falls die Auftragnehmerin verpflichtet ist, personenbezogene Daten nach dem Recht der Union oder des Mitgliedstaates, dem die Auftragnehmerin unterliegt, zu verarbeiten, wird die Auftragnehmerin den Auftraggeber hierüber vor der jeweiligen Verarbeitung schriftlich informieren, es sei denn, das Gesetz verbietet solche Informationen aus wichtigen Gründen des öffentlichen Interesses. Im letztgenannten Fall wird der Auftragnehmer den Verantwortlichen unverzüglich informieren, sobald ihm dies rechtlich möglich ist.

(3) Die Auftragnehmerin informiert den Auftraggeber unverzüglich, wenn sie der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Die Auftragnehmerin darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

(4) Die Auftragnehmerin kann Daten zur Nutzung der Software durch den Auftraggeber in anonymisierter Form zu Zwecken der Optimierung der Software, der Nutzererfahrung und für sicherheitsrelevante Auswertungen nutzen. Der Auftraggeber erteilt hiermit eine entsprechende Weisung für die entsprechende Anonymisierung.

4. Technische und organisatorische Maßnahmen

(1) Die Auftragnehmerin verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.

(2) Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist in **Anlage 2 zu dieser AVV** dokumentiert. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt der Auftragnehmerin vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Der Auftraggeber kann jederzeit eine aktuelle Übersicht der von der Auftragnehmerin getroffenen technischen und organisatorischen Maßnahmen anfordern.

5. Betroffenenrechte

(1) Die Auftragnehmerin unterstützt den Auftraggeber im Rahmen ihrer Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DSGVO (insb. Auskunft, Berichtigung, Sperrung oder Löschung). Soweit eine Mitwirkung der Auftragnehmerin für die Wahrung von

Betroffenenrechten durch den Auftraggeber erforderlich ist, wird die Auftragnehmerin die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen. Die Auftragnehmerin wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

(2) Auskünfte an Dritte oder den Betroffenen darf die Auftragnehmerin nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an sie gerichtete Anfragen wird sie unverzüglich an den Auftraggeber weiterleiten.

6. Sonstige Pflichten der Auftragnehmerin

(1) Die Auftragnehmerin unterrichtet den Auftraggeber unverzüglich, spätestens innerhalb von 48 Stunden, wenn ihr Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden.

(2) Im Zusammenhang mit der beauftragten Verarbeitung hat die Auftragnehmerin den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie erforderlichenfalls bei Durchführung einer Datenschutzfolgenabschätzung zu unterstützen. Alle erforderlichen Angaben und Dokumentationen sind dem Auftraggeber auf Anforderung unverzüglich zur Verfügung zu stellen.

(3) Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich die Auftragnehmerin, den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.

(4) Die bei der Auftragnehmerin zur Verarbeitung eingesetzten Personen haben sich schriftlich zur Vertraulichkeit verpflichtet, wurden mit den relevanten Bestimmungen des Datenschutzes vertraut gemacht und werden hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht.

(5) Die Auftragnehmerin wird den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihr zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten unterstützen.

(6) Die Auftragnehmerin hat eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz bestellt. In Zweifelsfällen kann sich der Auftraggeber direkt an den Datenschutzbeauftragten wenden (datenschutz@doo.net).

7. Rechte und Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.

(2) Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen bei der Auftragnehmerin in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme zu kontrollieren. Den mit der Kontrolle betrauten Personen ist von der Auftragnehmerin, soweit erforderlich und möglich, Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind. Kontrollen bei der Auftragnehmerin haben ohne vermeidbare Störungen ihres Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten der Auftragnehmerin, sowie nicht häufiger als alle 12 Monate statt.

8. Unterauftragnehmer

(1) Die Beauftragung von Unterauftragnehmern durch die Auftragnehmerin ist nur mit Zustimmung des Auftraggebers zulässig. Der Auftraggeber stimmt der Beauftragung von Unterauftragnehmern gemäß der Übersicht Unterauftragsverarbeiter von doo, abrufbar unter https://doo.net/de/about/rechtliches/downloads.html, zu. In der Übersicht Unterauftragsverarbeiter ist auch der Prozess für zukünftige Änderungen der Unterauftragsverarbeiter definiert.

(2) Die Auftragnehmerin hat die Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass diese die zwischen Auftraggeber und Auftragnehmerin getroffenen Vereinbarungen einhalten können. Die Auftragnehmerin hat insbesondere zu kontrollieren, dass sämtliche Unterauftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen haben.

(3) Nicht als Unterauftragsverhältnisse im Sinne diese AVV sind Dienstleistungen anzusehen, die die Auftragnehmerin bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit

auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die die Auftragnehmerin für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen und Bewachungsdienste.

(4) Die Beauftragung von Unterauftragsverarbeitern lässt die vertraglichen und datenschutzrechtlichen Verpflichtungen der Auftragnehmerin gegenüber dem Auftraggeber unberührt. Die Auftragnehmerin haftet für eventuelle Schlechtleistungen eines Unterauftragsverarbeiters wie für eigenes Verschulden.

9. Datenübermittlung in Drittländer

Die Auftragsverarbeitung findet auch in Drittländern statt. Die Übermittlung personenbezogener Daten an ein Drittland durch die Auftragnehmerin erfolgt dabei auf Basis eines Angemessenheitsbeschlusses gem. Art. 45 DSGVO und/oder auf Basis geeigneter Garantien gem. Art. 46 DSGVO (z.B. den von der Kommission erlassenen Allgemeinen Standardvertragsklauseln, die zwischen Auftragnehmerin und Unterauftragnehmern in Drittländern abgeschlossen wurden).

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Beendigung der Leistungsvereinbarung oder früher nach Aufforderung durch den Auftraggeber hat die Auftragnehmerin die im Auftrag verarbeiteten personenbezogenen Daten dem Auftraggeber auszuhändigen oder datenschutzgerecht zu löschen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

Anlage 1: Beschreibung der Auftragsverarbeitung

Verantwortliche Stelle

Der oben bezeichnete Auftraggeber ist verantwortliche Stelle und nutzt die Event-Management-Plattform der Auftragnehmerin.

Auftragsverarbeiter

Die Auftragnehmerin stellt dem Auftraggeber ihre Event-Management-Plattform als Software as a Service (SaaS) zur Verfügung.

Betroffene Personen

Die im Auftrag verarbeiteten personenbezogenen Daten betreffen folgende Kategorien betroffener Personen:

- 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 Auftraggebers als Teilnehmer in die Event-Management-Plattform transferiert wurden („Attendee Data“)

Kategorien von Daten

Die im Auftrag verarbeiteten personenbezogenen Daten gehören zu folgenden Datenkategorien:

- Name
- Adresse
- E-Mail-Adresse
- Bewegungsdaten auf Events („Session Tracking“)
- 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

Besondere Datenkategorien

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.

Gegenstand und Dauer der Verarbeitung

Die im Auftrag verarbeiteten personenbezogenen Daten werden verarbeitet zur Organisation und Durchführung von Events, einschließlich Einladung/Marketing, Anmeldung, Abrechnung, Teilnahme. Die Dauer der Verarbeitung entspricht, vorbehaltlich Ziffer 10 der AVV, der Laufzeit der Leistungsvereinbarung.

Anlage 2: Technisch und organisatorische Datensicherheitsmaßnahmen

Bei doo sind hinsichtlich der doo Event-Management-Plattform nachfolgende technische und organisatorische Maßnahmen der Datensicherheit i.S.d. Art. 32 DSGVO getroffen worden:

1. VERTRAULICHKEIT

1.1 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/

1.2 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 dem Personal von doo wird der Zugang zu den Administrationstools sichergestellt wie folgt:

- Zugang ist abgesichert durch ein Passwort mit Mindestlänge
- Zugang der Mitarbeiter wird über ACLs sichergestellt (Access Control Lists)
- Organisatorische Maßnahmen falls Mitarbeiter 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

1.3 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 dem Mitarbeiter nur Zugriff auf die Bereiche gewährt die er für seine Arbeit benötigt (Principle of least privilege). Weiterhin gibt es organisatorische Maßnahmen falls Mitarbeiter das Unternehmen verlassen (Löschen des Zugangs).

1.4 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.

1.5 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.

2. INTEGRITÄT

2.1 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.

2.2 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. Der Auftragnehmer 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 ist zertifiziert nach ISO 27001, so dass durch Backup-Systeme und ähnliche Mechanismen die Wahrscheinlichkeit für eine integritätsgefährdende Datendekoherenz sehr gering ist.

3. 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/

4. AUFTRAGSKONTROLLE

Im Rahmen der Auftragskontrolle gewährleistet doo, dass die im Auftrag zu verarbeitenden Daten nur entsprechend den in der Leistungsbeschreibung aufgeführten Weisungen verarbeitet werden.

Die Verfahrensweisen bei der Verarbeitung personenbezogener Daten sind vollständig und aktuell dokumentiert, so dass diese von einer externen Partei/dem Auftraggeber in zumutbarem Zeitaufwand nachvollzogen werden können.

Das Hosting der Server wird von AWS bereitgestellt. Dazu gibt es Verträge zwischen doo und AWS.

5. 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.

6. VERFAHREN ZUR REGELMÄSSIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

Bei doo ist ein Datenschutzmanagement implementiert und es ist ein betrieblicher Datenschutzbeauftragter benannt.

Es gibt eine Leitlinie zu Datenschutz und Informationssicherheit und Richtlinien, mit denen die Umsetzung der Ziele der Leitlinie gewährleistet wird. Die Leitlinien und Richtlinien werden regelmäßig im Hinblick auf ihre Wirksamkeit evaluiert und angepasst.

Es ist Datenschutz- und Informationssicherheits-Team (DST) eingerichtet, das Maßnahmen im Bereich von Datenschutz und Informationssicherheit plant, umsetzt, evaluiert und Anpassungen vornimmt.

Alle Mitarbeiter werden regelmäßig im Bereich Datenschutz und Informationssicherheit geschult. Es ist insbesondere sichergestellt, dass Datenschutzvorfälle von allen Mitarbeitern erkannt und unverzüglich dem DST gemeldet werden. Dieses wird den Vorfall sofort untersuchen. Soweit Daten betroffen sind, die im Auftrag von Kunden verarbeitet werden, wird Sorge dafür getragen, dass diese unverzüglich über Art und Umfang des Vorfalls informiert werden.