

Vertrag zur Auftragsverarbeitung (AV)

zwischen

Messe und Veranstaltungen GmbH Frankfurt (Oder)

Platz der Einheit 1
15230 Frankfurt (Oder)
Deutschland

als Auftraggeber und Verantwortlicher

– nachfolgend der „Verantwortliche“ –

Kontaktdaten der/des Datenschutzbeauftragten:

Name: Christian Türke
E-Mail: c.tuerke@muv-ffo.de

und

CTS EVENTIM Solutions GmbH

Contrescarpe 75a
28195 Bremen

als Auftragnehmer und Auftragsverarbeiter

– nachfolgend der „Auftragsverarbeiter“ –,

Kontaktdaten der/des Datenschutzbeauftragten:

Name: Thomas Voitke
E-Mail: datenschutz@eventim.de

zusammen nachfolgend die „Parteien“ und jeder von ihnen als „Partei“.

Präambel

Die vorliegende Vereinbarung zur Auftragsverarbeitung regelt die Anforderung an die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen im Zusammenhang mit der Erbringung der im Vertrag zwischen den Parteien vereinbarten Leistungen, auf den diesbezüglich verwiesen wird.

§ 1

Definitionen

AV	Diese Vereinbarung zur Auftragsverarbeitung.
Arten personenbezogener Daten	Zusammenfassung personenbezogener Daten zu Gruppen von Daten mit einem ähnlichen Verwendungszweck.
Auftragsverarbeiter	Die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle – wie oben angegeben und definiert – die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (Art. 4 Nr. 8 DS-GVO).
betroffene Person	Eine identifizierte oder identifizierbare natürliche Person; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann (Art. 4 Nr. 1 DS-GVO).
Dienstleistungen	Alle Dienstleistungen, die der Auftragsverarbeiter dem Verantwortlichen nach dem Vertrag zur Verfügung stellt.
Drittstaat	Staat, der weder Mitglied der Europäischen Union (EU) noch des Europäischen Wirtschaftsraums (EWR) ist.
DS-GVO	Datenschutz-Grundverordnung (Verordnung (EU) 2016/679).
Kategorien betroffener Personen	Zusammenfassung von betroffenen Personen zu einer Gruppe aufgrund deren im Wesentlichen gleichen Stellung bzw. Beziehung zum Verantwortlichen.
personenbezogene Daten	Alle Informationen, die sich auf eine betroffene Person beziehen (Art. 4 Nr. 1 DS-GVO).
TOM	Technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten vor unbeabsichtigter oder unrechtmäßiger Vernichtung oder unbeabsichtigter Löschung, Veränderung, unberechtigtem Zugriff oder unbeabsichtigter Offenlegung.

Verantwortlicher	Die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle – wie oben angegeben und definiert – die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art. 4 Nr. 7 DS-GVO).
Verarbeitung personenbezogener Daten	Jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung (Art. 4 Nr. 2 DS-GVO).
Vertrag	Der in der Präambel bezeichnete Vertrag.
Verletzung des Schutzes personenbezogener Daten	Eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden (Art. 4 Nr. 12 DS-GVO).

§ 2

Gegenstand und Laufzeit der AV

1. Diese AV legt die Rechte und Pflichten der Parteien in Bezug auf die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen zum Zwecke der Erbringung der Dienstleistungen fest.
2. Die Laufzeit dieser AV beginnt und endet mit der Laufzeit der Vereinbarung. Diese AV kann von beiden Parteien aus wichtigem Grund mit sofortiger Wirkung gekündigt werden. Die Kündigung bedarf mindestens der elektronischen Form.

§ 3

Zweck und Dauer der Verarbeitung / Kategorien betroffener Personen und Arten personenbezogener Daten

1. Zweck der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter ist die Erbringung der Dienstleistungen.
2. Die Verarbeitung personenbezogener Daten beginnt und endet mit der Laufzeit dieser AV, wie in § 2 Abs. 2 beschrieben. Die Datenverarbeitung, die zur Erfüllung von Löschungs- und/oder Rückgabeverpflichtungen gemäß § 8 erforderlich ist, bleibt hiervon unberührt.
3. Die Kategorien betroffener Personen sowie die Arten personenbezogener Daten, die im Auftrag verarbeitet werden, sind in **ANLAGE 1** näher beschrieben.

§ 4

Rechte und Pflichten des Verantwortlichen

1. Der Verantwortliche bleibt gegenüber den betroffenen Personen für die Einhaltung des Datenschutzes verantwortlich und stellt sicher, dass die Datenverarbeitung in Übereinstimmung mit den einschlägigen Bestimmungen des anwendbaren Datenschutzrechts erfolgt.
2. Zusätzlich zu den in dieser AV enthaltenen Anforderungen an Verarbeitung personenbezogener Daten kann der Verantwortliche den Auftragsverarbeiter Einzelweisungen über Art, Umfang und Ablauf der Datenverarbeitung, insbesondere über Berichtigung, Sperrung und Löschung erteilen. Diese Einzelweisungen sind in elektronischer Form oder in Textform zu erteilen.
3. Der Verantwortliche hat das Recht, die Einhaltung der Verpflichtungen aus dieser AV sowie etwaiger Einzelweisungen, insbesondere die Umsetzung der beschriebenen TOM des Auftragsverarbeiters auf Anfrage und mit zeitlich angemessener Vorankündigung in elektronischer Form oder in Textform zu überprüfen. Zu diesem Zweck wird der Auftragsverarbeiter dem Verantwortlichen, seinen Mitarbeitern oder bevollmächtigten Prüfern / Beratern, die durch eine seitens des Auftragsverarbeiters gestellte Verschwiegenheitsvereinbarung verpflichtet sind, nach zeitlich angemessener vorheriger Mitteilung in elektronischer Form oder in Textform durch den Verantwortlichen einen angemessenen Zugang zu den für den Verantwortlichen verarbeiteten Daten sowie den verwendeten Datenverarbeitungssystemen, Datenverarbeitungsprogrammen und relevanten Räumlichkeiten während der normalen Geschäftszeiten gewähren. Jede Partei trägt ihre eigenen Kosten, die aus einer solchen Überprüfung resultieren.

§ 5

Pflichten des Auftragsverarbeiters

1. Allgemeines

Der Auftragsverarbeiter darf personenbezogene Daten ausschließlich im Auftrag des Verantwortlichen gemäß den Anforderungen dieser AV und gemäß etwaiger Einzelweisungen des Verantwortlichen und ausschließlich zu den in dieser AV genannten Zwecken verarbeiten, es sei denn, der Auftragsverarbeiter ist zu einer hiervon abweichenden Verarbeitung personenbezogener Daten nach anwendbarem Recht verpflichtet (z.B. aufgrund einer behördlichen Anordnung). Im letzteren Fall wird der Auftragsverarbeiter den Verantwortlichen vor der Verarbeitung personenbezogener Daten zu diesem abweichenden Zweck über diese gesetzliche Verpflichtung informieren, es sei denn, dass das Gesetz eine solche Information aus wichtigen Gründen des öffentlichen Interesses verbietet.

2. Übermittlung ins Drittland

Die Datenverarbeitung erfolgt in einem Mitgliedstaat der Europäischen Union (EU) oder in einem Mitgliedstaat des Europäischen Wirtschaftsraums (EWR). Jede Übermittlung personenbezogener Daten in ein Drittland, einschließlich der Gewährung des Zugangs aus einem Drittland zu den in der EU/EWR gespeicherten personenbezogenen Daten, ist nur zulässig, wenn die Anforderungen der Artikel 44 ff. DS-GVO erfüllt sind, bevor personenbezogene Daten übertragen bzw. zugänglich gemacht werden und der Verantwortliche einer solchen Übermittlung vorher zustimmt. Die zum Zeitpunkt des Abschlusses dieser Vereinbarung vorhandenen Empfänger in einem Drittland, an die personenbezogene Daten übermittelt werden bzw. die Zugriff auf in der EU/EWR gespeicherte personenbezogene Daten haben, werden zusammen mit den jeweils getroffenen Garantien zur Sicherstellung eines angemessenen Datenschutzniveaus im betreffenden Drittland in **ANLAGE 2** aufgeführt.

3. Verarbeitungsverzeichnis

Der Auftragsverarbeiter ist verpflichtet, ein schriftliches oder elektronisches Verzeichnis aller Verarbeitungstätigkeiten bezogen auf die personenbezogenen Daten entsprechend den gesetzlichen Vorgaben zu führen und es auf dem aktuellen Stand zu halten.

4. TOM (Technische und organisatorische Maßnahmen)

Der Auftragsverarbeiter wird angemessene TOM treffen, um die Sicherheit der Datenverarbeitung zu gewährleisten. Dabei sind der Stand der Technik, die Durchführungskosten, die Art, der Umfang und die Zwecke der Verarbeitung personenbezogener Daten sowie die Eintrittswahrscheinlichkeit und die Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen. Die derzeit vom Auftragsverarbeiter getroffenen TOM werden in **ANLAGE 3** beschrieben. Die TOM unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insofern ist es zulässig, dass der Auftragsverarbeiter die beschriebenen TOM ändert, solange das bestehende Sicherheitsniveau der definierten Maßnahmen dabei insgesamt nicht reduziert wird. Ungeachtet dessen sind Änderungen zu dokumentieren und dem Verantwortlichen mitzuteilen, z.B. durch die regelmäßige Bereitstellung einer aktualisierten Liste von TOM. Wesentliche Änderungen der TOM bedürfen der Vereinbarung in mindestens elektronischer Form.

5. Vertraulichkeit

Der Auftragsverarbeiter ist zur Vertraulichkeit verpflichtet und stellt sicher, dass alle Personen, die zur Verarbeitung personenbezogener Daten des Verantwortlichen im Sinne dieser AV befugt sind, sich zur Vertraulichkeit verpflichtet haben oder einer entsprechenden gesetzlichen Verschwiegenheitspflicht unterliegen. Insbesondere ist eine Offenlegung personenbezogener Daten untersagt; dies gilt nicht soweit und solange hierzu eine Verpflichtung nach anwendbarem Recht besteht.

6. Überwachung

Während der gesamten Vertragslaufzeit überwacht der Auftragsverarbeiter die Einhaltung der Bestimmungen dieser AV und ggf. der Einzelweisungen, die der Verantwortliche gemäß § 4 Abs. 2 erteilt.

7. Kommunikation

Soweit im Einzelfall erforderlich, erfolgt sämtliche Kommunikation zwischen dem Verantwortlichen und dem Auftragsverarbeiter unter zusätzlichen Sicherheitsmaßnahmen (z.B. Verschlüsselung der elektronischen Kommunikation). Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Prüfungstätigkeiten oder sonstige Kontrollmaßnahmen der Datenschutzaufsichtsbehörden, soweit sie sich auf die Verarbeitung personenbezogener Daten im Rahmen dieser AV beziehen.

8. Unterstützung des Verantwortlichen

Unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützt der Auftragsverarbeiter den Verantwortlichen so weit wie möglich bei der Erfüllung seiner datenschutzrechtlichen Pflichten (z.B. Meldung von Datenschutzverletzungen an die Datenschutzbehörden und die betroffenen Personen gemäß §6, Durchführung von Datenschutzverträglichkeitsprüfungen sowie Beantwortung von Anfragen zur Ausübung der Rechte der betroffenen Personen). Wendet sich eine betroffene Person mit einem Antrag zur Wahrnehmung datenschutzrechtlicher Betroffenenrechte (z.B. Berichtigung, Löschung oder Einschränkung der Verarbeitung ihrer personenbezogenen Daten) direkt an den Auftragsverarbeiter, leitet dieser den Antrag unverzüglich an den Verantwortlichen weiter.

9. Verstoß gegen das Datenschutzrecht

Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich informieren, wenn seiner Meinung nach eine Weisung des Verantwortlichen gegen geltendes Datenschutzrecht verstößt. Der Auftragsverarbeiter ist dann berechtigt, die Ausführung der betreffenden Weisung solange auszusetzen, bis der Verantwortliche sie bestätigt oder ändert.

10. Der Datenschutzbeauftragte

Der Auftragsverarbeiter hat einen Datenschutzbeauftragten bestellt, soweit dies gesetzlich erforderlich ist.

§ 6

Meldung einer Verletzung des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten des Verantwortlichen benachrichtigt der Auftragsverarbeiter den Verantwortlichen unverzüglich (in der Regel per E-Mail oder telefonisch den Datenschutzbeauftragten des Verantwortlichen), nachdem er Kenntnis von einer Verletzung des Schutzes personenbezogener Daten erlangt hat.

§ 7

Kontrolle

Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die erforderlich sind, um die Einhaltung der in dieser AV festgelegten Verpflichtungen des Auftragsverarbeiters, insbesondere die Implementierung angemessener TOM, nachzuweisen. Zu diesem Zweck gestattet der Auftragsverarbeiter auch Überprüfungen-, einschließlich Inspektionen, unter den in § 4 Abs. 3 genannten Bedingungen.

§ 8

Beendigung und Löschung

Der Auftragsverarbeiter wird alle unter dieser AV verarbeiteten personenbezogenen Daten und alle Kopien davon nach 30 Tagen nach der Beendigung dieser AV löschen, es sei denn, das anwendbare Recht verlangt eine weitere Speicherung der personenbezogenen Daten (z.B. Aufbewahrungspflichten). Im letzteren Fall hat der Auftragsverarbeiter dafür Sorge zu tragen, dass die Datenverarbeitung auf diesen Zweck beschränkt bleibt. Auf eine in elektronischer Form oder in Textform getätigte Aufforderung des Verantwortlichen innerhalb von 30 Tagen nach der Beendigung dieser AV wird der Auftragsverarbeiter alle unter dieser AV verarbeiteten personenbezogenen Daten und alle Kopien davon an den Verantwortlichen gegen Vergütung der damit verbundenen Aufwände zurückgeben.

§ 9

Unterauftragnehmer

1. Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragsverarbeiter z.B. als Telekommunikationsleistungen, Post- / Transportdienstleistungen, Wartung und Benutzerservice sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Verantwortlichen auch bei ausgelagerten Nebenleistungen angemessene Maßnahmen zu ergreifen.
2. Der Verantwortliche erteilt hiermit seine Zustimmung zur Beauftragung der in **ANLAGE 4** aufgeführten Unterauftragnehmer. Jede Beauftragung von Unterauftragnehmern, die nicht in **ANLAGE 4** enthalten

sind, bedarf der vorherigen Zustimmung (in elektronischer Form oder in Textform) des Verantwortlichen, die nicht ohne wichtigen Grund verweigert werden darf.

Die vorherige Zustimmung des Verantwortlichen gilt als erteilt, wenn a) der Auftragsverarbeiter die geplante Inbetriebnahme eines neuen Unterauftragnehmers dem Verantwortlichen in elektronischer Form oder in Textform mitgeteilt hat, b) der Verantwortliche nicht binnen sieben Werktagen nach Erhalt der Mitteilung in elektronischer Form oder in Textform widersprochen hat und c) der Auftragsverarbeiter mit dem jeweiligen Unterauftragnehmer zum Zeitpunkt der Durchführung der Auftragsverarbeitung einen Vertrag zur Auftragsverarbeitung nach Maßgabe des § 9 Abs. 3 abgeschlossen hat.

3. Der Auftragsverarbeiter hat mit den Unterauftragnehmern Verträge zur Auftragsverarbeitung abzuschließen, die so ausgestaltet sind, dass sie dem Datenschutzniveau dieser AV entsprechen. Der Verantwortliche hat das Recht, auf Anfrage (in elektronischer Form oder in Textform) vom Verarbeiter Informationen über die Umsetzung der Datenschutzverpflichtungen im Rahmen des Untervertragsverhältnisses zu erhalten.
4. Wenn ein Unterauftragnehmer eine Verarbeitung personenbezogener Daten in oder aus einem Drittland erbringen soll, muss der Auftragsverarbeiter die Rechtmäßigkeit der Übermittlung personenbezogener Daten in das Drittland gemäß Art. 44 ff. DS-GVO sicherstellen. Der betreffende Unterauftragnehmer und die entsprechende Garantie zur Sicherstellung eines angemessenen Datenschutzniveaus sind in **ANLAGE 2** aufzunehmen.
5. Kommt ein Unterauftragnehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten dieses Unterauftragnehmers.

§ 10

Abschließende Regelungen

1. Die nachfolgenden Anlagen sind integraler Bestandteil dieser AV:
 - ANLAGE 1: Kategorien betroffener Personen und Arten personenbezogener Daten**
 - ANLAGE 2: Übermittlung von personenbezogenen Daten in Drittländer**
 - ANLAGE 3: TOM**
 - ANLAGE 4: Liste mit genehmigten Unterauftragnehmern**
2. Änderungen oder Ergänzungen dieser AV bedürfen zu ihrer Wirksamkeit mindestens der elektronischen Form. Dies gilt auch für Änderungen der gegenständlichen Regelung.
3. Alle Streitigkeiten oder Ansprüche, die sich aus oder im Zusammenhang mit dieser AV ergeben, unterliegen deutschem Recht. Ausschließlicher Gerichtsstand ist beim sachlich zuständigen Gericht am Geschäftssitz des Auftragsverarbeiters.
4. Für den Fall, dass eine oder mehrere Bestimmungen dieser AV ganz oder teilweise unwirksam sein sollten oder werden, wird die Gültigkeit und Durchsetzbarkeit der übrigen Bestimmungen dieser AV dadurch nicht berührt. Gleiches gilt für den Fall, dass der Vertrag Lücken enthält. Eine unwirksame bzw. fehlende Bestimmung ist durch eine solche zu ersetzen, die, soweit rechtlich zulässig, dem tatsächlichen oder mutmaßlichen Willen der Parteien am nächsten kommt, sofern sie diese berücksichtigt hätten.

Frankfurt (Oder),

Bremen,

Unterschrift Auftraggeber

Unterschrift CTS EVENTIM Solutions GmbH

ANLAGE 1

Kategorien betroffener Personen und Arten personenbezogener Daten

Die Verarbeitung personenbezogener Daten im Rahmen dieser AV betrifft die folgenden Kategorien betroffener Personen und die folgenden Arten personenbezogener Daten:

Kategorien betroffener Personen	Arten personenbezogener Daten
<p>Interessenten und Käufer für Produkte, Dienstleistungen und Eintrittskarten für Veranstaltungen des Verantwortlichen</p> <p>Mitarbeiter des Verantwortlichen und des Auftragsverarbeiters</p>	<p>Bei den nachstehenden Daten kann es sich aufgrund der Konfigurationsmöglichkeit des Systems um optionale oder freiwillige Angaben seitens der Kunden des Auftraggebers handeln:</p> <p>Kennzeichen Privatperson/ Firmenkunde, Merkmale/Attribute und Merkmalsgruppen, Anrede, Titel, Branche, Namen, Adresse(n), Hausnummer, Zusatz zur Hausnummer, Zusatz zur Adresse, Land, Postleitzahl, Ort, Ortsteil, E-Mail, Telefonnummer(n), Anredetext, Geburtstag, Geschlecht, Sprache, USt.-ID, Notizen, Aliasname(n), Zahlungsmodus, Zahlungsart, Bankverbindung, Standardzustellweg, Mitglied im Fanclub, Eintritts- und Austrittsdatum, Austrittsgrund, Mandatsreferenz, SEPA-Gläubiger-ID, Newsletter-Anmeldungen, IP-Adresse, Tracking-Informationen</p>

ANLAGE 2

Übermittlung von personenbezogenen Daten in Drittländer

Die folgende Liste enthält Empfänger von personenbezogenen Daten in Drittländern, die direkt oder indirekt an der Verarbeitung personenbezogener Daten, die unter diese AV fallen, beteiligt sind sowie die jeweils zur Anwendung kommenden Garantien zur Sicherstellung eines angemessenen Datenschutzniveaus gemäß Art. 44 ff. DS-GVO.

Name und Adresse des Empfängers im Drittland	Rechtfertigung der Datenübermittlung / Geeignete Garantien (z. B. Angemessenheitsbeschluss der EU-Kommission, Abschluss EU-Standardvertragsklauseln, Binding Corporate Rules etc.)
Nicht anwendbar	Nicht anwendbar

ANLAGE 3

TOM (Technische und organisatorische Maßnahmen)

Die nachfolgenden Maßnahmen gelten nur im Falle des Systembetriebs durch den Auftragnehmer in dessen Rechenzentrum (sog. ASP-Lösung).

*Sofern der Systembetrieb durch den Auftraggeber selbst erfolgt (sog. Onsite-Lösung) gelten im Rahmen dieser Vereinbarung nur die mit * gekennzeichneten Maßnahmen. Alle anderen erforderlichen Maßnahmen sind in diesem Fall vom Auftraggeber selbst durchzuführen.*

1. Maßnahmen zur Sicherstellung der Vertraulichkeit der Systeme und Dienste (Art. 32 Abs. 1 lit. b DS-GVO)

a) Zutrittskontrolle

Vorgabe / Anforderung:

Ein unbefugter Zutritt zu Datenverarbeitungsanlagen ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.

Vom Auftragnehmer konkret getroffene Maßnahmen:

- Ausweiskontrolle sowie Tragepflicht von Berechtigungsausweisen
- Beschränkung der Vergabe von Ausweisen, Schlüsselkarten etc.
- Dokumentation der Vergabe und Rückgabe von Schlüsselkarten etc.
- Pförtner, z. B. Personenkontrolle
- Schlüsselregelung
- Sicherheitsschlösser
- Manuelles Schließsystem
- System für Zutrittsberechtigungen für Mitarbeiter und Dritte
- Videoüberwachung der Eingänge
- Protokollierung der Besucher
- Sorgfältige Auswahl von Hilfspersonal, z. B. Reinigungskräften, Wachpersonal
- Schutz durch Sicherheitsfirmen außerhalb der Geschäftszeiten

b) Zugangskontrolle

Vorgabe / Anforderung:

Eine Nutzung der Datenverarbeitungssysteme durch Unbefugte ist zu verhindern.

Vom Auftragnehmer konkret getroffene Maßnahmen:

- Erstellung und Verwendung von Benutzerprofilen auf Personenebene
- Zuordnung von Benutzerrechten
- Passwortrichtlinie inkl. Mindestlänge, Mindestanforderungen an Passwörter:
 - Müssen mindestens acht Zeichen lang sein
 - Müssen mindestens je ein Zeichen aus den Kategorien Großbuchstaben von A bis Z, Kleinbuchstaben von a bis z, Ziffern der Basis 10 (0 bis 9) sowie Sonderzeichen (z. B. !, \$, #, %) enthalten
- Authentifikation mit persönlicher Benutzerkennung und Passwort
- Einsatz von VPN-Technologie
- Einsatz einer dem Stand der Technik entsprechenden Software-Firewall
- Einsatz einer dem Stand der Technik entsprechende Anti-Viren-Software
- Einsatz von Intrusion-Detection-Systemen
- Verschlüsselung von Smartphone-Inhalten
- Automatische Bildschirmsperre
- Session Timeout für inaktive Sessions nach einem festgelegten Zeitraum

c) Zugriffskontrolle

Vorgabe / Anforderung:

Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Vom Auftragnehmer konkret getroffene Maßnahmen:

- Erstellung eines differenzierten Berechtigungskonzepts, Freigabe der Daten nur für Befugte (Need-to-know- und Least-Privilege-Prinzip)
- Verwaltung der Zugriffsrechte durch Administrator
- Anzahl der Personen mit „Administrator-Status“ minimiert
- Authentifizierung durch Benutzername und Passwort
- Protokollierung der Zugriffe
- Zeitnahe Sperrung der Konten ausgeschiedener Mitarbeiter
- Einsatz von Aktenvernichtern und Protokollierung der Vernichtung
- Sichere Aufbewahrung von Datenträgern
- Löschung von Datenträgern nach Verwendung
- Regelmäßige Anwendung von Sicherheits-Patches
- Trennung von Produktion und Entwicklung

d) Trennungskontrolle

Vorgabe / Anforderung:

Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.

Vom Auftragnehmer konkret getroffene Maßnahmen:

- Trennung von Produktiv- und Testsystem, Sandboxing, physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Erstellung eines Berechtigungskonzepts
- Nachweislich logische Trennung der Daten der jeweiligen Kunden des (Unter-) Auftragnehmers, d. h. Daten verschiedener verantwortlicher Stellen und/oder (Unter-) Auftragnehmers sind getrennt zu verarbeiten und gegenseitiger Zugriff ist auszuschließen

2. Maßnahmen zur Sicherstellung der Integrität der Systeme und Dienste (Art. 32 Abs. 1 lit. b DS-GVO)

a) Weitergabekontrolle

Vorgabe / Anforderung:

Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Vom Auftragnehmer konkret getroffene Maßnahmen:

- * Verschlüsselte Datenübertragungen
- * Der Zugriff auf extern bereitgestellte Services erfolgt über verschlüsselte Protokolle (https, sftp etc.)
- Virtual Private Networks (VPN)
- Verschlüsselung von Datenträgern vor Versand
- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- Sollte eine Verschlüsselung nachweislich nicht möglich sein, muss ein sicheres Alternativverfahren durchgeführt werden (z. B. verschließbare Transportbehälter)
- * Weitergabe von Daten an Dritte ist lediglich mit Zustimmung des Verantwortlichen in mindestens elektronischer Form
- Sorgfältige Auswahl von Transportpersonal und -fahrzeugen beim physischen Transport von Daten

b) Eingabekontrolle

Vorgabe / Anforderung:

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.

Vom Auftragnehmer konkret getroffene Maßnahmen:

- Richtlinien zu Eingabe und Erfassung von Daten
- 4-Augen-Prinzip
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf der Basis eines detaillierten Berechtigungskonzepts
- Protokollierung der Eingabe

3. Maßnahmen zur Sicherstellung der Verfügbarkeit und Belastbarkeit der Systeme und Dienste (Art. 32 Abs. 1 lit. b und c DS-GVO)

a) Verfügbarkeitskontrolle

Vorgabe / Anforderung:

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

Vom Auftragnehmer konkret getroffene Maßnahmen:

- Erstellung eines Backup- und Recovery-Konzepts
- Monitoring und Überwachung des Systemzustands und Meldung von Fehlfunktionen
- Test der Datenwiederherstellung aus Backup
- Unterbrechungsfreie Stromversorgung (USV)
- Aufbewahrung der Datensicherung an einem sicheren Ort
- Einsatz einer dem Stand der Technik entsprechender Anti-Viren-Software
- Einsatz einer dem Stand der Technik entsprechender Software-Firewall
- Einsatz einer dem Stand der Technik entsprechender Hardware-Firewall
- Sicherheitskonzept für Serverräume einschließlich Notfallpläne
- Überwachung der Temperatur und Feuchtigkeit in Serverräumen
- Alarmsystem, Feuer- und Rauchmelder für Serverräume
- Feuerlöschgeräte in Serverräumen
- Keine Serverräume unter sanitären Anlagen
- Physische Redundanz der Datenverarbeitungssysteme

b) Rasche Wiederherstellung

Vorgabe / Anforderung:

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

Vom Auftragnehmer konkret getroffene Maßnahmen:

- Redundante Datenspeicherung
- Cloud-Services
- Doppelte Infrastruktur

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der TOM (Art. 32 Abs. 1 lit. d DS-GVO)

a) Auftragskontrolle

Vorgabe / Anforderung:

Die weisungsgemäße Auftragsdatenverarbeitung ist zu gewährleisten.

Vom Auftragnehmer konkret getroffene Maßnahmen:

- Incident-Response-Management
- * Vertragliche Regelung der Zusammenarbeit zwischen Auftraggeber und (Unter-) Auftragnehmer
- * Sorgfältige Auswahl von Auftragnehmern
- * Kontrolle der technischen und organisatorischen Maßnahmen beim (Unter-) Auftragnehmer
- Vereinbarung von Stichprobenkontrollen (z. B. bei Änderungen, turnusmäßig)
- Vereinbarung von Vertragsstrafen bei Verstößen
- * Sicherstellung von Datenrückgabe/-löschung
- * Regelmäßige Schulungen der Mitarbeiter zum Datenschutz (Schulungspflicht)

b) Sonstige Überprüfungsmaßnahmen

- Regelmäßige Self-Assessments als Bestandteil eines PDCA-Zyklus (Plan-Do-Check-Act-Zyklus)
- Entwicklung eines Sicherheitskonzepts
- Regelmäßige Auditierung, Prüfungen (auch durch Externe)
- Fortlaufende Zertifizierungen

ANLAGE 4

Liste mit genehmigten Unterauftragnehmern

Unterauftragnehmer aus der CTS EVENTIM-/KPS-Gruppe

CTS EVENTIM AG & Co. KGaA 1)

Contrescarpe 75a

28195 Bremen

CTS EVENTIM Solutions GmbH 1)

Contrescarpe 75a

28195 Bremen

KPS Payment GmbH & Co. KG 2)

Contrescarpe 75A

28195 Bremen

KPS Interactive Media GmbH & Co. KG 2) 3)

Contrescarpe 75A

28195 Bremen

Ticket Online Sales & Service GmbH 2) 3)

Ludwigsluster Straße 33

19370 Parchim

Weitere Unterauftragnehmer:

TeleCash GmbH & Co. KG

Marienbader Platz 1

61348 Bad Homburg, Deutschland

1) Sofern nicht selbst Auftragsverarbeiter

2) Bei Nutzung von Callcenter- und Serviceleistungen und/oder Service-Webshops mit Durchführung des Payments

3) Bei Nutzung von Callcenter- und Serviceleistungen