Vertrag zur Verarbeitung von personenbezogenen Daten **Stand: Juli 2020**

im Auftrag der

Aussteller der hier eingeloggt hat.

(im Folgenden: Auftraggeber)

durch die

spring Messe Management GmbH
Am Friedensplatz 3
68165 Mannheim
(nachfolgend .Auftragnehmer" genannt)

1. Gegenstand und Dauer des Vertrags

Der Auftraggeber beauftragt den Auftragnehmer mit folgenden datenschutzrechtlich relevanten Tätigkeiten im Bereich der Datenverarbeitung:

Betrieb der Lead Management System im Rahmen der Zukunft Personal und gilt mit dem Hauptvertrag als Anmeldung /Buchung eines Messestands für die Veranstaltungsdauer.

(1) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind insbesondere folgende Datenarten/-kategorien:

- Vorname, Nachname
- Firma
- Anschrift
- Kommunikationsdaten (ggf. Telefonnummer, E-Mail-Adresse)

(2) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Messebesucher des Auftraggebers
- Beschäftigte/Mitarbeiter des Auftraggebers
- Ansprechpartner der vorgenannten Kategorien betroffener Personen

(3) Vertragslaufzeit

Der Vertrag beginnt mit der Auftragsbestätigung/Bestellung und endet automatisch, ohne dass es einer Kündigung bedarf nach der Veranstaltung.

(4) Auftragsinhalt

Der Auftragnehmer übermittelt, die zum Zeitpunkt der Ticketregistrierung erfassten Daten, soweit diese mitgeteilt wurden, dem Auftraggeber, wenn der Besucher zur Datenverarbeitung für die Lead Management Nutzung vor Ort eingewilligt hat. Durch diese Einwilligung, erlaubt der Besucher dem Unterauftragnehmer, seine Daten zu übermitteln. Die verifizierbarenVerantwortlichen seitens Auftraggeber haftet für die Einwilligung. (siehe Anlage 2).

2. Weisungsbefugnis / Ansprechpartner

Der Auftragnehmer verarbeitet Daten ausschließlich nach Maßgabe des mit dem Auftraggeber geschlossen Vertrags. Der Auftragnehmer behält sich vor die Daten, die von der Ticketregistrierung erhoben worden sind, u.a. für statistischen Zwecke zu nutzen.

Weisungsberechtigt auf der Seite des Auftraggebers ist:

Der Standleiter, im Falle eines nicht vorhanden sein, der in Anmeldung angegebene Ansprechpartner.

Für die Annahme von Weisungen auf der Seite des Auftragnehmers sind zuständig:

Seitens spring: der jeweilige Mitarbeiter der Abteilung Messeproduktion
E-Mail: operations@messe.org

Seitens Unterauftragnehmer: Firma FairVerify Event Solutions GmbH, Industriestraße 21-23 69245 Bammental, Tim Haymann,
E-Mail: info@fairverify.de

Bei einem Wechsel oder einer dauerhaften Verhinderung des verantwortlichen Ansprechpartners ist dies durch den jeweiligen Vertragspartner unverzüglich schriftlich unter Benennung eines Vertreters mitzuteilen.

Weisungen des Auftraggebers bedürfen mindestens der Textform.

Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

Datenschutzbeauftragte von spring

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Datenschutzbeauftragte:

Name: Ralf Bayer

E-Mail: datenschutz@messe.org

b) Die Datenschutzbeauftragte stellt die Ausführungen des Bundesdatenschutzgesetzes, der Datenschutz-Grundverordnung sowie andere Vorschriften über den Datenschutz im Hinblick auf das Auftragsverhältnis seitens der Auftragnehmer sicher. Hierzu führt sie regelmäßige Kontrollen durch. Über die Kontrollen ist ein Protokoll anzufertigen. Stellt die Datenschutzbeauftragte im Rahmen ihres Aufgabenkreises Unregelmäßigkeiten bei der Datenverarbeitung fest, so informiert sie unverzüglich die Geschäftsführung von der Auftragnehmer. Ein Wechsel der Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

Meldung bei der Aufsictitsbehörde

Der Auftragnehmer ist bei der zuständigen Aufsichtsbehörde gemeldet und registriert.

Zuständige Aufsichtsbehörde für den Datenschutz ist:

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg
Königstraße 10a
70173 Stuttgart

Der Auftraggeber ist berechtigt bei der Aufsichtsbehörde jederzeit Einsicht in die der den Auftragnehmer betreffende Registereintragung zu nehmen bzw. Informationen über die aktuellen Registereintragungen über den Auftragnehmer zu verlangen.

(1) Der Auftragnehmer hat alle im Rahmen des Auftrages überlassenen Unterlagen, Dokumente und andere Informationsträger sowie alle Informationen, die der Auftragnehmer bei Durchführung des Auftrages zur Kenntnis gelangen, absolut vertraulich zu behandeln. Diese Verpflichtung gilt während und auch nach Beendigung des Vertrages.

(2) Der Auftragnehmer und jede unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der aus diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind. Der

Auftragnehmer gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben. Der Auftragnehmer sichert zu, bei der Durchführung der Arbeiten nur Beschäftigte einzusetzen, die auf die Verpflichtung auf Vertraulichkeit schriftlich verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden.

Technisch-organisatorische Maßnahmen:

(1) Der Auftragnehmer stellt die Sicherheit (Art. 28 Abs. 3 lit. c, 32 DS-GVO, insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO) her. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Ver fügbarkeit sowie der Belastbarkeit der Systeme. Dabei wird der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen (Art. 32 Abs. 1 DS-GVO) berücksichtigt (Anlage 1).
(2) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es den Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

Berichtigung, Löschung von Daten, Einschränkungen der Verarbeitung

(1) Nach der Veranstaltung werden die Daten den Auftraggeber übermittelt. Ab der Übermittlung übernimmt die Auftraggeber die volle Verantwortung für alle Rechte und Pflichten bezüglich der Betroffenenrechte (Art. 12-23 DS-GVO). spring wird den Auftraggeber bei der Erfüllung von Pflichten gegenüber den Betroffenen unterstützen.

(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) Der Unterauftragnehmer des Auftragnehmers die Firma FairVerify Event Solutions GmbH zur Datenverarbeitung überlassenen Daten nicht anderweitig verwenden die im Zusammenhang mit dem Auftragsverhältnis stehen. Des Weiteren vernichtet diese Daten automatisiert sechs Wochen nach Auftragsende (Übermittlung der Daten).

Unterauftragsverhältnisse

(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, der Auftragnehmer z. B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.
(2) Der Auftragnehmer wird den Unterauftragnehmer (weiterer Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen. Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber der Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt. Zu diesem Vertrag aufgeführten Unterauftragnehmer gelten mit Unterzeichnung des Vertrages die Zustimmung des Auftraggebers als erteilt.
(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher . Gleiches gilt, wenn der Unterauftragnehmer im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen schriftlichen Zustimmung des Auftraggebers (mind. Textform). In diesem Fall stellt der Auftragnehmer sicher, dass sämtliche in dieser Vereinbarung getroffenen Regelungen von weiteren Unterauftragnehmern eingehalten werden.

Durchführung von Lead Management
FairVerify Event Solutions GmbH
Industriestraße21-23
69245 Bammental

Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.
(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

Mitteilung bei Verstößen von dem Auftragnehmer

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen und vorherige Konsultationen.
Hierzu gehören u. a.
a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
c) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die auf ein Fehlverhalten des Auftraggebers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen. Im Übrigen erfolgen die Unterstützungsleistungen durch den Auftragnehmer unentgeltlich.

Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragsnehmers - bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt.
(2) Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zum Datenschutz den Regelungen des Vertrages vor.
(3) Sollten einzelne Bestimmungen dieses Vertrages unwirksam oder undurchführbar sein oder nach Vertragsschluss unwirksam oder undurchführbar werden, bleibt davon die Wirksamkeit des Vertrages im Übrigen unberührt. An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll diejenige wirksame und durchführbare Regelung treten, deren Wirkungen der datenschutzrechtlichen und wirtschaftlichen Zielsetzung am nächsten kommen, die die Vertragsparteien mit der unwirksamen bzw. undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich der Vertrag als lückenhaft erweist.
(4) Es gilt deutsches Recht. Gerichtsstand für alle Streitigkeiten aus diesem Vertrag ist Mannheim.
(5) Vertragssprache ist deutsch.

Folgende Anlagen sind Bestandteil des Vertrages:

Anlage 1: **Verfahrensübergreifende Datenschutzmaßnahmen gemäß Art. 32 DSGVO**
Anlage 2: **Beschreibung Lead-App**
Anlage 3: **Kommunikation versus Auftraggeber via Mail**

Anlage 1

Verfahrensübergreifende Datenschutzmaßnahmen gemäß Art. 32 DSGVO

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

1.1. Zutrittskontrolle

Der Auftragnehmer sichert zu, den Zugang zu den Datenverarbeitungsanlagen durch folgende Verfahren abzusichern:

- Zutrittsregelung für betriebsfremde Personen; die Umsetzung erfolgt z. B. durch
  – Protokollierung der Zu- und Abgänge von betriebsfremden Personen
  – Ausgabe von Besucherausweisen
  – Aufenthalt von Fremden im Unternehmensgebäude nur in Anwesenheit von Mitarbeitern
  – Rücknahme von Zugangsmitteln nach Ablauf der Berechtigung
- Zutrittsregelung für betriebsangehörige Personen; die Umsetzung erfolgt z. B. durch
  – Protokollierung der Zu- und Abgänge von Mitarbeitern
  – Traspondersystem
- Festlegung der zutrittsberechtigten Personen für Rechner-/Serverraum
- Maßnahmen, damit nur Befugte Zutritt zum Rechner- /Serverraum erhalten
- Bereitstellung verschließbarer Schränke/Rollcontainer für Mitarbeiter
- Schlüsselregelung
- Objektsicherung

1.2 Zugangs und Zugriffskontrolle

Der Auftragnehmer gewährleistet, dass nur autorisierte Mitarbeiter Zugriff zu den verarbeiteten Daten haben. Der Auftragnehmer gewährleistet weiter, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Hierfür werden folgende Sicherungsmechanismen verwendet:

- Authentisierung der Benutzer gegenüber dem Datenverarbeitungssystem. d.h. Identifikation durch Benutzernamen und Kennwort oder 2-Faktor-Verfahren
- Regelungen zur Passwortvergabe
  – Persönliches Passwort
  – Mindestens 10 Zeichen, darunter auch Groß- und Kleinbuchstaben und Zahlen; unter 12 Zeichen auch Sonderzeichen;
  – Vergabe durch Nutzer selbst
  – Zugangssperre nach fünf Fehlversuchen
  – Keine Weitergabe an Dritte
  – Vertretungsregelung für Fall der Abwesenheit (Urlaub, Krankheit etc.)
  – Sperre der zuletzt verwendeten 5 Passworte
- Umgehende Sperrung von Berechtigungen beim Ausscheiden von Mitarbeitern
- Separate Benutzerkennungen für administrative Zwecke
- Regelmäßige Kontrolle der Gültigkeit von Berechtigungen (jährlich)
- Sicherung der Bildschirmarbeitsplätze bei Abwesenheit und laufendem System (Passwortschutz für Bildschirmschoner nach 5 Min.)
- Automatisierte temporäre Sperrung von Benutzerkonten bei mehrfachen fehlerhaften Anmelde-versuchen.
- Abschottung interner Netze gegen Zugriffe von außen (Firewall, Verschlüsselung VPN)
- Abschottung von Serversystemen mittels Firewalls
- Erstellung eines Benutzerprofils

d.h. Festlegung von Zugriffsberechtigungen hinsichtlich personenbezogener Daten von Nutzern

- Vergabe von Berechtigungen an Mitarbeiter und Erfüllungsgehilfen nach dem Minimalprinzip; Zugriff auf Anwendungen und Systemkomponenten wird nur gestattet, wenn dieser Zugriff für die konkrete Tätigkeit erforderlich ist.
- Erstellung eines Berechtigungskonzeptes
  – Einrichtung von Administrationsrechten
  – Verwaltung der Zugriffsrechte durch Systemadministrator
- Trennung von Test- und Produktionsbetrieb

- Vergabe von Berechtigungen muss nachvollziehbar dokumentiert werden und einen Genehmigungsschritt umfassen.
- datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger nach dem jeweiligen Stand der Technik unter Beachtung der jeweils gültigen Normen (DIN 66399:2012) oder Beauftragung eines auf Entsorgung von Datenträgern spezialisierten Dienstleisters mit der Entsorgung, der die Daten¬träger mit derselben oder einer höheren Sicherheitsstufe vernichten wird. Die zur Entsorgung vorge¬sehenen Datenträger sind während der Lagerung und des Transports mit geeigneten Maßnahmen vor unbefugtem Zugriff zu schützen.
- datenschutzgerechte Entsorgung von Makulatur (beispielsweise Fehldrucke von Arbeitslisten, Anschreiben etc.) mittels eines Aktenvernichters der eine nach DIN 66399:2012 definierten Sicherheitsstufe P-4 aufweist, oder Beauftragung eines auf Aktenvernichtung spezialisierten Dienstleister mit der Entsorgung, der die Dokumente mit derselben oder einer höheren Sicherheitsstufe vernichten wird.

1.3 Zugriffstrennung
Der Auftragsnehmer gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt voneinander verarbeitet werden.

Datentrennung logisch auf Anwenderebene

- Berechtigungskonzept mit Festlegung der Zugriffsrechte
- Mandantenfähige Datenbank

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

2.1. Weitergabekontrolle

Der Auftragnehmer gewährleistet, dass bei der elektronischen Übertragung von Daten diese 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. Die auftragsgemäß zu verarbeitenden Daten werden mit Hilfe von folgenden Einrichtungen zur Datenübertragung zwischen den Vertragsparteien ausgetauscht:

- Dokumentation von Datenempfänger, der Transport- /Übermittlungswege, der zur Übermittlung von Daten befugten Personen und der zu übermittelnden Daten
- Authentisierte und hinreichend verschlüsselte Übertragung von Daten vor der Weitergabe bei nicht gesicherten Übertragungswegen

2.2 Eingabekontrolle

- Führung von nachweisbar erteilten Zugriffsberechtigungen
- Protokollierung von Eingabe, Veränderungen oder Löschung personenbezogener Daten
- Regelung zu Zugriffsbefugnissen auf erstellte Protokolldaten
- Löschungsregelung für Protokolldaten

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

3.1. Verfügbarkeitskontrolle

Der Auftragnehmer gewährleistet, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- unterbrechungsfreie Stromversorgung (USV)
- CO2 Feuerlöschgerät im/vor Serverraum
- Sicherung der Datenbestände durch Erstellung eines Bestandssicherungskonzeptes
- Rekonstruktion von Datenbeständen; Testläufe bei der Rekonstruktion von Datenbeständen
- Vertretungsregelungen für Mitarbeiter

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

4.1 Datenschutz- Management
Der Auftragenehmer gewährleistet die systematische Planung und Konzeption, Umsetzung, Kontrolle, Überwachung sowie Optimierung der Anforderungen an den Datenschutz.

4.2 Incident-Response Management

4.3 Gewährleistung datenschutzfreundlicher Voreinstellungen bei Gestaltung und Betrieb der Datenverarbeitungsprozesse, z. B. durch:
– informationelle Gewaltentrennung innerhalb und zwischen verantwortlichen Stellen
– Reduzierung von Möglichkeiten der Kenntnisnahme vorhandener Daten
– Bevorzugung von automatisierten Verarbeitungsprozessen (nicht Entscheidungsprozesse), die eine Kenntnisnahme verarbeiteter Daten entbehrlich machen und die Einflussnahme gegenüber im Dialog gesteuerten Prozessen begrenzen
– Implementierung automatischer Sperr- und Löschroutinen
– Regelungen zur Kontrolle von Prozessen zur Änderung von Verfahren
• weitreichende Pseudonymisierung und Verschlüsselung personenbezogener Daten
• Meldung von Sicherheitsvorfällen, die im laufenden Betrieb sichergestellt werden
• Kontrolle der Wirksamkeit der durchgeführten Maßnahmen mindestens einmal pro Jahr
• sichere und ausreichende Default-Einstellung für die Server, durch die ein abgesicherter Wiederanlauf des Serversystems in der vorgesehenen Zeit durchgeführt werden kann.

4.4 Auftragskontrolle (bei Tätigkeit als Auftragsverarbeiter und Einschaltung von weiteren Unterauftragnehmer)

Der Auftragnehmer gewährleistet dabei die weisungsgemäße Auftragsdatenverarbeitung im Unternehmen und bei weiteren Auftragsverarbeitern (Unterauftragnehmer) durch:
• Kontrolle der Einhaltung von Datensicherheitsbestimmungen durch Auftragnehmer und Meldung, wenn Verstöße vorliegen oder der Verdacht besteht, dass die Datensicherheitsvorgaben unzureichend sind.
• Verpflichtung der Mitarbeiter des Auftragnehmers zur Wahrung der datenschutzrelevanten Vorgaben
• Erteilung von Weisungen an die Mitarbeiter und Unterauftragnehmer hinsichtlich der vorgesehenen Verwendung der Daten, die für die Auftragsdurchführung erforderlich sind und verwendet werden sollen.
- Strenge Auswahl des Unterauftragnehmers und formalisiertes Auftragsmanagement (Policy)

Anlage 2 – Beschreibung Lead-App

„Der Besucher hat die Möglichkeit, sich vom Aussteller scannen zu lassen und seine Daten somit über die, von FairVerify Event Solutions GmbH verwaltete, Lead App an den Aussteller weiterzugeben.

In diesem Fall bestätigt der Besucher die Kenntnisnahme der Datenschutzerklärung auf dem jeweiligen Gerät.

Sofern der Besucher diese Form der Datennutzung ablehnt, endet der Prozess - es werden keine Daten in das Portal des Auftraggebers übertragen.“

Anlage 3 – Kommunikation versus Auftraggeber via Mail

„…Wir möchten Sie an dieser Stelle auch auf den sensiblen Umgang mit den erfassten Daten hinweisen. Laut **DSGVO** ist eine Einwilligung des Besuchers bzgl. der Nutzung seiner personenbezogenen Daten zwingend erforderlich.
Als Aussteller stehen Sie hier in der Pflicht, die entsprechenden Regularien & gesetzlichen Vorgaben einzuhalten. Hierzu ist es empfehlenswert Ihre Datenschutzerklärung ausgedruckt zur Messe mitzunehmen und diese auf Anfrage dem Betroffenen auszuhändigen.
Ferner haben wir ein Pop-up programmiert, dass sowohl Sie als Aussteller als auch die Besucher während der Erfassung noch einmal explizit auf die damit verbundene Datennutzung hinweist. Wir empfehlen diesen Hinweis aktiv seitens Besucher bestätigen zu lassen.

Erfolgt eine Bestätigung, werden die Daten in Ihr Portal übertragen.
Sofern der Besucher diese Form der Datennutzung ablehnt, endet der Prozess - es werden keine Daten in Ihr Portal übertragen.
Gerne stehen wir Ihnen im Vorfeld der Messe für Rückfragen weiterhin per E-Mail (operations@messe.org) oder den unten aufgeführten Kontaktdaten zur Verfügung.
Für kurzfristige Anliegen vor Ort steht Frau Sina Blottenbeg im Foyer Eingang am Infocounter für Sie bereit.“