Leistungsvertrag
über die
Übermittlung Daten aus Scan2Lead oder aus papiergestützten Erfassungsbögen an Gesundheitsbehörden

zwischen

der Messe Düsseldorf GmbH, Stockumer Kirchstr. 61, Messeplatz, 40474 Düsseldorf, vertreten durch die Geschäftsführung,

- nachfolgend „Auftragnehmer“ genannt -

und

Aussteller des CARAVAN SALON 2020

- nachfolgend „Vertragspartner“ genannt –

Präambel

Die Messe Düsseldorf ist Betreiberin des Messegeländes in Düsseldorf. Dort und andernorts weltweit veranstaltet sie Messen, Ausstellungen und Kongresse. Eine dieser Veranstaltungen ist der CARAVAN SALON 2020. Messe Düsseldorf hält die Rechte an dieser Veranstaltung.

Der Vertragspartner nimmt als Aussteller am CARAVAN SALON 2020 teil. Dies ist per gesonderter Verträge geregelt.

Dieser Vertrag spielt insbesondere dann eine Rolle, wenn ein Austeller auf seinem Stand während des CARAVAN SALON unter anderem auch Bewirtung jeglicher Art anbietet und entweder das Scan2Lead-System zur Erfüllung seiner Pflichten nach der Coronaschutzverordnung Nordrhein-Westfalen (CoronaSchVO NRW) (Rückverfolgbarkeit) gebucht hat oder diese Verpflichten papiergestützt erfüllt.

Dies vorausgeschickt schließen die Parteien vorliegende Vereinbarung.

§ 1
Vertragsgegenstand

Ziel dieser Vereinbarung ist die Bündelung der Beantwortung von Anfragen von Gesundheitsbehörden im Zusammenhang mit der Rückverfolgbarkeit nach CoronaSchVO NRW.

§ 2
Leistungen Messe Düsseldorf

(1) Im Falle einer behördlichen Anfrage erteilt die Messe Düsseldorf der anfragenden Behörde in den Grenzen des geltenden Rechts (insbesondere des Datenschutzrechts) eine entsprechende Auskunft.

(2) Im Falle der Nutzung des Scan2Lead-Systems durch den Vertragspartner bewahrt die Messe Düsseldorf Telefonnummer, Aufenthaltsdauer für vier Wochen auf. Sodann erfolgt die Löschung dieser Daten

(3) Die Messe Düsseldorf bewahrt die vom Aussteller papiergestützt erhobenen sämtlichen Daten für vier Wochen auf. Sodann erfolgt die Löschung dieser Daten.

(4) Vorstehende Leistungen sind abgegolten mit der gesondert vereinbarten Gebühr für die Messeteilnahme.

§ 3
Obliegenheiten / Mitwirkung Aussteller

(1) Es obliegt dem Vertragspartner die gewissenhafte Erfassung der Besucher entweder per Scan2Lead oder per Papier.

(2) Falls der Vertragspartner die Erfassung auf Papier durchführt, wird er der Messe Düsseldorf am Schluss eines jeden Messetages sämtliches Erfassungsbögen in der Messeleitung im Original aushändigen (in der Regel an einen Hallenläufer des Auftragnehmers).

(3) Im Falle dessen, dass Behörden im Zusammenhang mit der Rückverfolgbarkeit nach CoronaSchVO NRW eine Anfrage unmittelbar an den Vertragspartner richten, wird dieser die Behörde an die Messe Düsseldorf zur zentralen Bearbeitung der Anfrage verweisen.

§ 4
Datenschutz

(1) Die Parteien verpflichten sich zur Einhaltung der in der Bundesrepublik Deutschland und der Europäischen Union jeweils geltenden gesetzlichen Bestimmungen des Datenschutzes. Die Parteien werden die Daten nur für den vertraglichen Zweck verarbeiten. Es ist ihnen untersagt, die Daten an Dritte weiterzugeben oder Dritten zugänglich zu machen. Diese Pflichten gelten auch nach Vertragsende.

(2) Die Vertragsparteien schließen zur Einhaltung der einschlägigen gesetzlichen datenschutzrechtlichen Bestimmungen einen Auftragsdatenverarbeitungsvertrag nach Art. 28 Datenschutzgrundverordnung (Verordnung (EU) 2016/679 (nachstehend „DSGVO“ genannt)), der zu dem hier vorliegenden Vertrag als **Anlage** genommen wird.

(3) Die Vertragsparteien verpflichten sich mit der Unterschrift unter den Vertrag die Datenvertraulichkeit nach Maßgabe des Gesetzes zu wahren. Diese Verpflichtung werden die Parteien nachweisbar auch ihren Mitarbeitern und Beauftragten auferlegen und die Einhaltung überwachen.

(4) Wenn und soweit die Messe Düsseldorf zur Durchführung dieses Vertragsverhältnisses personenbezogene Daten von Organen, Mitarbeitern, Erfüllungsgehilfen oder sonstigen Beauftragten des Vertragspartners verarbeitet, so wird der Vertragspartner den vorgenannten betroffenen Personen von der Messe Düsseldorf nach ihrem Ermessen erstellte und zur Verfügung gestellte Datenschutzhinweise aushändigen (digital oder in Papierform).

§ 5
Loyalität / Unterrichtung

(1) Beide Vertragsparteien werden sich gegenseitig umgehend über alle Umstände, die für die Durchführung dieses Vertrages von Bedeutung sein könnten, unterrichten. Maßnahmen mit Öffentlichkeitswirkung sind nach Möglichkeit zuvor mit der jeweils anderen Vertragspartei abzustimmen.

(2) Beide Vertragspartner verpflichten sich gegenseitiges Stillschweigen über Geschäfts-, Betriebs- und Redaktionsgeheimnisse gegenüber Dritten zu bewahren. Dies gilt auch nach einer eventuellen Beendigung der Kooperation.

§ 6
Haftungsausschluss, Erfüllungsinteresse

(1) Messe Düsseldorf schließt gegenüber dem Vertragspartner jegliche Haftung für einen Schaden aus, der auf einer schuldhaften Pflichtverletzung der Messe Düsseldorf, eines gesetzlichen Vertreters, Erfüllungsgehilfen oder sonstigen Beauftragen der Messe Düsseldorf beruht, soweit dies gesetzlich zulässig ist.

(2) Der Vertragspartner haftet über die Erbringung seiner geschuldeten Leistung hinaus nicht für eine etwaige Nichterreichung der von Messe Düsseldorf mit der Eingehung dieses Vertrags verfolgten kommunikativen Ziele, es sei denn der Vertragspartner hat deren Erreichung durch schuldhafte Verletzung wesentlicher vertraglicher Pflichten bzw. durch grob fahrlässiges Verhalten erschwert oder vereitelt.

(3) Die Vertragsparteien stimmen überein, dass Messe Düsseldorf weder an der Organisation noch an der Durchführung der Veranstaltung beteiligt ist, hierfür keine Verantwortung trägt und dritten gegenüber, insbesondere Teilnehmern, Besuchern und Lieferanten der Veranstaltung nicht haftet.

§ 7
Rechtsfolgen bei Ausfall der Veranstaltung / Kündigung

(1) Findet die Veranstaltung nicht statt, so werden beide Parteien von ihren vertraglichen Primär- und Sekundärpflichten frei. Bereits erbrachte Leistungen sind zurückzugewähren. Jede Partei trägt ihre Kosten selbst. Dies gilt nicht, wenn und soweit eine der Vertragsparteien den Ausfall der Veranstaltung zu vertreten hat. In diesem Fall ist diejenige Partei, die den Ausfall der Veranstaltung zu vertreten hat, der jeweils anderen Partei gegenüber ersatzpflichtig.

(2) Jede Vertragspartei ist berechtigt, den Vertrag aus wichtigem Grund fristlos und schriftlich zu kündigen. Ein wichtiger Grund liegt insbesondere vor, wenn die andere Vertragspartei schuldhaft gegen ihr obliegende wesentliche vertragliche Verpflichtungen verstößt oder ein Verhalten an den Tag legt, dass die Zweckrichtung dieses Vertrages untergräbt, und den Verstoß trotz schriftlicher Abmahnung nicht innerhalb einer angemessenen Frist abstellt. Einer vorherigen Abmahnung bedarf es nicht, wenn sie zwecklos ist oder der zur Kündigung berechtigten Vertragspartei nicht zumutbar ist.

§ 8
Schlussbestimmungen

(1) Der Aussteller ist sich seiner Eigenschaft als Verantwortlicher im datenschutzrechtlichen Sinne nach Art. 4 Nr. 7 DSGVO bewusst. Die Messe Düsseldorf weist diesbezüglich auf die den Aussteller treffenden Informationspflichten nach Art. 12 ff. DSGVO und die in der Regeln bestehende Notwendigkeit einer diesbezüglichen Rechtsberatung (ggfls. per online gestützter Legal Tech Lösungen) hin.

(2) Die Laufzeit dieses Vertrages beginnt mit seiner Unterzeichnung und endet mit Ablauf des Schlusstages des CARAVAN SALON 2020 spätestens mit Ablauf des 30. September 2020 – je nachdem was früher eintritt – , ohne dass es dazu einer weiteren Erklärung durch die Parteien bedarf.

(3) Alle Entgelte nach diesem Vertrag sind Nettoentgelte, neben denen die Umsatzsteuer in der jeweils gesetzlich festgesetzten Höhe ausgewiesen wird und zu entrichten ist.

(4) Erfüllungsort und Gerichtsstand ist Düsseldorf. Es gilt das Recht der Bundesrepublik Deutschland.

(5) Nebenabreden auch mündlicher Art zu diesem Vertrag bestehen nicht. Änderungen und Ergänzungen des Vertrages bedürfen der Schriftform. Dies gilt auch für die Änderung dieses Schriftformerfordernisses.

(6) Sollten einzelne Bestimmungen dieses Vertrages unwirksam sein oder werden, so sollen die übrigen Bestimmungen hiervon unberührt bleiben. Die sich möglicherweise ergebende Lücken sollen so ausgefüllt werden, dass Sinn und Zweck des Vertrages erhalten bleiben.

Anlage

Vertrag über Datenverarbeitung im Auftrag, Art. 28 EU-DSGVO

zwischen

Messe Düsseldorf GmbH, Stockumer Kirchstr. 61, Messeplatz, 40474 Düsseldorf, vertreten durch die Geschäftsführung,

- nachfolgend „Auftragnehmer“ genannt -

und

dem im Leistungsvertrag bezeichneten Vertragspartner

- nachfolgend „Auftraggeber“ genannt –

§ 1
Allgemeines

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag und auf Weisung des Auftraggebers i.S.d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO). Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.

(2) Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

§ 2
Gegenstand des Auftrags

Der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen umfassen Folgendes:

(a) Scan2Lead – Rückverfolgbarkeit nach Coronaschutzverordnung Nordrhein-Westfalen (CoronaSchVO NRW):

(aa) Zweck der Datenverarbeitung: Einhaltung der Verpflichtungen zur Ermöglichung der Rückverfolgbarkeit nach der CoronaSchVO NRW.

(bb) Regelmäßig verarbeitete Datenarten:

Namen, postalische Anschrift, Telefonnummer und den Zeitraum des Aufenthalts auf dem Messestand.

(cc) Kategorien betroffener Personen:

Besucher auf dem Messestand.

§ 3
Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Dem Auftragnehmer steht nach Ziff. 4 Abs. 5 das Recht zu, den Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.

(2) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen.

(3) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

(4) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Auftraggeber geltenden gesetzlichen Meldepflicht besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

(5) Auf Anfrage teilt der Auftraggeber dem Auftragnehmer die Kontaktdaten der / des betrieblichen Datenschutzbeauftragten in Textform mit.

§ 4
Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilter dokumentierter Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschließlich nach diesem Vertrag und/oder den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat.

(2) Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des Auftraggebers verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind.

(3) Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

§ 5
Datenschutzbeauftragter des Auftragnehmers

Auf Anfrage teilt der Auftragnehmer dem Auftraggeber die Kontaktdaten der / des betrieblichen Datenschutzbeauftragten in Textform mit. Die Kontaktdaten der / des betrieblichen Datenschutzbeauftragten des Auftragnehmers sind zudem auf der Internetseite des Auftragnehmers unter www.messe-duesseldorf.de/datenschutz zu ersehen.

§ 6
Meldepflichten des Auftragnehmers

Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei der Umsetzung der Meldepflichten unterstützen.

§ 7
Mitwirkungspflichten des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12-23 DSGVO. Es gelten die Regelungen von Ziff. 11 dieses Vertrages.

(2) Der Auftragnehmer wirkt an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten durch den Auftraggeber mit. Er hat dem Auftraggeber die insoweit jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

(3) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten.

§ 8
Kontrollbefugnisse

(1) Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer im erforderlichen Umfang zu kontrollieren. Die Kontrolle des Auftragnehmers kann auch durch Einholung einer Selbstauskunft beim Auftragnehmer erfolgen. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen.

(2) Im Hinblick auf die Verpflichtung zur Folgenabschätzung des Auftraggebers vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags, stellt der Auftragnehmer sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen laut Art. 32 EU DSGVO überzeugen kann. Hierzu weist der Auftragnehmer dem Auftraggeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen gemäß Art. 32 EU DSGVO und der Anlage zu diesem Vertrag nach. Dabei kann der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, – nach Wahl des Auftragnehmers – auch durch Vorlage eines aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit erbracht werden.

(3) Der Auftraggeber kann eine Einsichtnahme in die vom Auftragnehmer für den Auftraggeber verarbeiteten Daten sowie insoweit in die verwendeten Datenverarbeitungssysteme und -programme verlangen.

(4) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen.

§ 9
Unterauftragsverhältnisse

(1) Dem Auftraggeber ist die Beauftragung nachstehender Unterauftragnehmer durch den bekannt.

adventics GmbH
Pilgersheimer Straße 62
81543 München, Deutschland
Tel.: +49 89 4444 33 111
E-Mail: contact@scan2lead.com

(2) Der Auftragnehmer hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann.

(3) Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten.

(4) Der Auftragnehmer hat mit dem Unterauftragnehmer einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Darüber hinaus hat der Auftragnehmer dem Unterauftragnehmer dieselben Pflichten zum Schutz personenbezogener Daten aufzuerlegen, die zwischen Auftraggeber und Auftragnehmer festgelegt sind.

(5) Nicht als Unterauftragsverhältnisse i.S.d. Absätze 1 bis 6 sind Dienstleistungen anzusehen, die der Auftragnehmer 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 der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. Der Auftragnehmer ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten. Die Wartung und Pflege von IT-System oder Applikationen stellt ein zustimmungspflichtiges Unterauftragsverhältnis und Auftragsverarbeitung i.S.d. Art. 28 DSGVO dar, wenn die Wartung und Prüfung solche IT-Systeme betrifft, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden und bei der Wartung auf personenbezogenen Daten zugegriffen werden kann, die im Auftrag des Auftraggebers verarbeitet werden.

§ 10
Vertraulichkeitsverpflichtung

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Der Auftraggeber ist verpflichtet, dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitzuteilen.

(2) Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragnehmer sichert ferner zu, dass er seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und zur Vertraulichkeit verpflichtet hat. Der Auftragnehmer sichert ferner zu, dass er insbesondere die bei der Durchführung der Arbeiten tätigen Beschäftigten zur Vertraulichkeit verpflichtet hat und diese über die Weisungen des Auftraggebers informiert hat.

(3) Die Verpflichtung der Beschäftigten nach Absatz 2 sind dem Auftraggeber auf Anfrage nachzuweisen.

§ 11
Geheimhaltungspflichten

(1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

(2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

§ 12
Vergütung

Die Vergütung des Auftragnehmers wird gesondert vereinbart.

§ 13
Technische und organisatorische Maßnahmen zur Datensicherheit

(1) Der Auftragnehmer 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 als **Anlage 3** zu diesem Vertrag beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Voraus mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

(3) Der Auftragnehmer wird die von ihm getroffenen technischen und organisatorischen Maßnahmen regelmäßig und auch anlassbezogen auf ihre Wirksamkeit kontrollieren. Für den Fall, dass es Optimierungs- und/oder Änderungsbedarf gibt, wird der Auftragnehmer den Auftraggeber informieren.

§ 14
Vertragslaufzeit

(1) Dieser Vertrag ist mit seiner Bestätigung durch den Auftragnehmer geschlossen. Er endet – ohne dass es dazu einer gesonderten Erklärung bedarf – mit dem Wegfall des Zwecks der Datenverarbeitung im Auftrag. Dieser Zweckfortfall tritt mit dem Ende der Datenverarbeitung zu den in § 2 genannten Leistungen ein. .

§ 15
Beendigung

Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt.

Anlage

Technische und organisatorische Maßnahmen des Auftragnehmers
Der Auftragnehmer trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

• Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren

Technische Maßnahmen	Organisatorische Maßnahmen
Chipkarten / Transpondersysteme	Schlüsselregelung / Liste
Manuelles Schließsystem	Empfang / Rezeption / Pförtner
Sicherheitsschlösser	Besucherbuch / Protokoll der Besucher
Absicherung der Gebäudeschächte	Mitarbeiter- / Besucherausweise
Türen mit Knauf Außenseite	Besucher in Begleitung durch Mitarbeiter
Videoüberwachung der Eingänge	Sorgfalt bei Auswahl des Wachpersonals
	Sorgfalt bei Auswahl Reinigungsdienste

• Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können. Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint

Technische Maßnahmen	Organisatorische Maßnahmen
Login mit Benutzername + Passwort	Verwalten von Benutzerberechtigungen
Anti-Viren-Software Server	Erstellen von Benutzerprofilen
Anti-Virus-Software Clients	Zentrale Passwortverwaltung
Firewall	Richtlinie „Sicheres Passwort“
Intrusion Detection Systeme	Richtlinie „Löschen / Vernichten“
Mobile Device Management	Allg. Richtlinie Datenschutz und / oder Sicherheit
Einsatz von VPN bei Remote-Zugriffen	Mobile Device Policy
Verschlüsselung von Smartphones	Anleitung „Manuelle Desktopsperre“
BIOS Schutz (separates Passwort)	
Automatische Desktopsperre	
Verschlüsselung von Notebooks / Tablet	

• Zugriffskontrolle

Maßnahmen, die 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.

Technische Maßnahmen	Organisatorische Maßnahmen
Externer Aktenvernichter (DIN 66399)	Einsatz Berechtigungskonzepte
Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	Minimale Anzahl an Administratoren
	Verwaltung von Benutzerrechte durch Administratoren

- **Trennungskontrolle**

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden

Technische Maßnahmen	Organisatorische Maßnahmen
Trennung von Produktiv- und Testumgebung	Steuerung über Berechtigungskonzept
Logische Trennung (Systeme / Datenbanken / Datenträger) bei virtualisierten Systemen	Festlegung von Datenbankrechten
Mandantenfähigkeit relevanter Anwendungen	

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

- **Weitergabekontrolle**

Maßnahmen, die 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.

Technische Maßnahmen	Organisatorische Maßnahmen
Einsatz von VPN	Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
Bereitstellung über verschlüsselte Verbindungen wie sftp, https	Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen

- **Eingabekontrolle**

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Technische Maßnahmen	Organisatorische Maßnahmen

Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
Manuelle oder automatisierte Kontrolle der Protokolle	Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)
	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
	Klare Zuständigkeiten für Löschungen

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

- **Verfügbarkeitskontrolle**

  Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Technische Maßnahmen	Organisatorische Maßnahmen
Feuer- und Rauchmeldeanlagen	Backup & Recovery-Konzept (ausformuliert)
Feuerlöscher Serverraum / Löschanlage	Kontrolle des Sicherungsvorgangs
Serverraumüberwachung Temperatur und Feuchtigkeit	Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
Serverraum klimatisiert	Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
USV	Existenz eines Notfallplans (z.B. BSI IT-Grundschutz 100-4)
Schutzsteckdosenleisten Serverraum	Getrennte Partitionen für Betriebssysteme und Daten
RAID System / Festplattenspiegelung	
Videoüberwachung Serverraum-Eingänge	

- **Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)**

  Maßnahmen, die gewährleisten, dass nach einer Betriebsstörung Systeme und Daten schnell wiederhergestellt werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
Zweites Rechenzentrum auf Gelände Messe Düsseldorf	
Datenspiegelung (Metrocluster)	
Halbstündige Snapshots als Wiederherstellungsmöglichkeit von gelöschten oder veränderten Daten	

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

- **Datenschutz-Management;**

Technische Maßnahmen	Organisatorische Maßnahmen

Zentrale Dokumentation aller Verfahrensanweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (Intranet)	Bestellung eines internen betrieblichen Datenschutzbeauftragter (DSB)
Anderweitiges dokumentiertes Sicherheits-Konzept	Mitarbeiter geschult und auf Vertraulichkeit / Datengeheimnis verpflichtet
Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	Regelmäßige Sensibilisierung der Mitarbeiter mindestens jährlich
	Beauftragung eines externen Informationssicherheitsbeauftragter (ISB)
	Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
	Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach

- **Incident-Response-Management**

Aufgeführt sind alle Maßnahmen, die die Reaktion auf Sicherheitsverletzungen unterstützen

Technische Maßnahmen	Organisatorische Maßnahmen
Einsatz von Firewall und regelmäßige Aktualisierung	Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Daten-Pannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
Einsatz von Spamfilter und regelmäßige Aktualisierung	Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
Einsatz von Virenscanner und regelmäßige Aktualisierung	Einbindung von DSB und ISB in Sicherheitsvorfälle und Datenpannen
Intrusion Detection System (IDS)	Dokumentation von Sicherheitsvorfällen und Datenpannen via E-Mail / Ticketsystem in Planung
Intrusion Prevention System (IPS)	Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

- **Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)**

Privacy by design / Privacy by Default.

Technische Maßnahmen	Organisatorische Maßnahmen
Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	
Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen	

- **Auftragskontrolle**

  Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung.

Technische Maßnahmen	Organisatorische Maßnahmen
	Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
	Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit
	Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln
	Schriftliche Weisungen an den Auftragnehmer
	Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
	Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht
	Vereinbarung wirksamer Kontrollrechtgegenüber dem Auftragnehmer
	Regelung zum Einsatz weiterer Subunternehmer
	Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
	Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus