Vertrag über Datenverarbeitung im Auftrag nach Art. 28 der Verordnung (EU) 2016/679 EU-DSGVO

sowie

über die Übermittlung personenbezogener Daten in Drittländer (2004/915/EG)

zwischen

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

- nachfolgend „Auftragnehmer“ oder „Datenexporteur“ genannt -

und

dem Vertragspartner (Firma und Anschrift s. Anmeldeunterlagen),

- nachfolgend „Auftraggeber“ oder „Datenimporteur“ genannt –

ABSCHNITT A - ALLGEMEINES

Präambel

Der Auftragnehmer ist Betreiber des Messegeländes in Düsseldorf, Deutschland. Hier und an anderen Veranstaltungsorten weltweit richtet er Messe, Ausstellungen und Kongresse aus. Im Zuge dessen bietet der Auftragnehmer verschiedene digitale Dienstleistungen an, die die Verarbeitung personenbezogener Daten nach sich ziehen.

Der Auftraggeber ist Aussteller bei einer vom Auftraggeber ausgerichteten Veranstaltung.

Dies vorausgeschickt schließen die Parteien folgende Vereinbarung. Diese greift, wenn und insoweit eine entsprechende Leistungsvereinbarung besteht.

§ 1
Allgemeines

(1) Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung personenbezogener Daten.

(2) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag und auf Weisung des Auftraggebers i.S.d. Art. 4 Nr. 8 und Art. 28 DSGVO. Diese Beauftragung bezieht sich – sofern der Auftraggeber dies im Rahmen seines Messeauftritts per gesonderter Bestellung geordert bzw. durch Nutzung in Anspruch genommen hat – auf die Dienstleistungen:

- Matchmaking,

- Aussteller Personalerfassung,
- Besucher Einladungen und / oder
- Einladung in das Online Order System (OOS) und Einladung in die Funktion eines weiteren Ansprechpartners zur Messeorganisation.

Abschnitt B dieses Vertrages enthält einen sich auf diese Beauftragung beziehenden Auftragsverarbeitungsvertrag nach Maßgabe des Art. 28 DSGVO. Die Begriffsbedeutungen innerhalb dieses Abschnitts B richten sich nach den Regelungen des Art. 4 DSGVO.

(3) Vorbehaltlich entsprechender gesonderter Bestellungen der Leistungen

- Besuchergutscheine und / oder
- Scan2Lead

findet je nach Standort des Datenimporteurs ein Datenexport in Drittländer statt. Der sich hierauf beziehende Abschnitt C dieses Vertrages regelt diesbezüglich das Nähere nach Maßgabe von EU-Standardvertragsklauseln nach der Entscheidung der EU Kommission 2004/915/EG.

ABSCHNITT B – Auftrags(daten)verarbeitung

§ 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) Matchmaking:

(aa) Zweck der Datenverarbeitung: Der Auftragnehmer bietet eine digitale Networking-Plattform mit Namen „Grip“ an, auf der Nachfrager und Anbieter von Waren und Dienstleistungen auf Basis der bei individueller Anmeldung angegebenen Daten zueinander finden können. Auf Basis von Übereinstimmungen der vorgenannten Kriterien oder aufgrund von Ähnlichkeiten mit anderen Personen innerhalb der Networking-Plattform werden dem Nutzer für ihn potentiell interessante Kontakte vorgeschlagen, die er mit Hilfe einer App oder einer Desktopversion davon kontaktieren kann. Der Auftraggeber übermittelt an den Auftragnehmer personenbezogene Daten, damit dieser die betroffenen Personen zur Teilnahme an der Networking-Plattform auffordern kann.

(bb) Regelmäßig verarbeitete Datenarten: Name, Vorname, Foto (soweit zur Verfügung gestellt), E-Mailadresse, berufliche Position, Brancheninformationen, Interessen, Informationen über das Produkt- oder Dienstleistungsportfolio.

(cc) Kategorien betroffener Personen: Besucher und Aussteller einschließlich deren Mitarbeitern, Organen und sonstigen Beauftragten sowie Mitarbeitern, Organen und sonstigen Beauftragten der an der Messebeteiligung des Auftraggebers in sonstiger Weise beteiligten Unternehmen.

(b) Aussteller Personalerfassung:

(aa) Zweck der Datenverarbeitung: Der Auftragnehmer erfasst Personen, die zur Laufzeit einer Veranstaltung auf dem Messestand des Auftraggebers tätig sind. Der Auftraggeber übermittelt

an den Auftragnehmer personenbezogene Daten dieser Personen, damit dieser die betroffenen Personen dazu auffordern kann, sich als Aussteller-Personal erfassen zu lassen. Zur besseren Abwicklung des Messeauftritts des Auftraggebers spricht der Auftragnehmer erfasste Personen zu Dienstleistungen und themenverwandten Folgeveranstaltungen sowie zu Kommunikationsservices wie Matchmaking (§ 2 Buchstabe a)) und Scan2Lead (§ 15 Abs. 2 Buchstabe b)) an.

(bb) Regelmäßig verarbeitete Datenarten: Name, Vorname, Foto (soweit zur Verfügung gestellt), E-Mailadresse, berufliche Position, Brancheninformationen, Interessen.

(cc) Kategorien betroffener Personen: Daten von Ausstellern einschließlich deren Mitarbeitern, Organen und sonstigen Beauftragten sowie Mitarbeitern, Organen und sonstigen Beauftragten der an der Messebeteiligung des Auftraggebers in sonstiger Weise beteiligten Unternehmen.

(c) Besucher-Einladungen:

(aa) Zweck der Datenverarbeitung: Der Auftragnehmer bietet eine Dienstleistung an, im Rahmen derer der Auftraggeber Listen mit E-Mail Adressen seiner Kunden, die als potentielle Besucher einer vom Auftragnehmer durchgeführten Messe / Ausstellung, an der der Auftraggeber als Aussteller teilnimmt, in Betracht kommen, an den Auftragnehmer übermittelt. Der Auftragnehmer verschickt sodann Eintrittskartengutscheine an die angegebenen E-Mail Adressen, um diese zur jeweiligen Veranstaltung einzuladen. Diese Dienstleistung verfolgt den Zweck, es dem Aussteller bzw. dem mit ihm verbundenen Unternehmen zu erleichtern, Eintrittskartengutscheine an seine Kunden zu verschicken, weil er diese nicht zunächst beim Auftragnehmer erwerben und sodann in einem zweiten Schritt selbst an seine Kunden versenden muss.

(bb) Regelmäßig verarbeitete Datenarten: Vorname, Name und E-Mail Adresse.

(cc) Kategorien betroffener Personen: aus Sicht des Auftraggebers potentieller Messebesucher sowie Mitarbeiter, Organe und sonstige Beauftragte der an der Messebeteiligung des Auftraggebers beteiligten Unternehmen.

(d) Einladung in das Online Order System (OOS) und Einladung in die Funktion eines weiteren Ansprechpartners zur Messeorganisation:

(aa) Zweck der Datenverarbeitung:

Der Auftragnehmer bietet ein sog. Online Order System (OOS) an. Dort kann der Auftraggeber Zusatzleistungen für seinen Messeauftritt bestellen. Der im Rahmen der Anmeldung zur Messeteilnahme des Auftraggebers in der Standanmeldung benannte Ansprechpartner beim Auftraggeber hat in seinem OOS-Account die Möglichkeit, andere Personen als zusätzliche Nutzer innerhalb seines Standauftrages einzuladen. Zur Einladung eines anderen Nutzers muss der Einladende die E-Mail Adresse des einzuladenden weiteren Nutzers in das OOS eingeben. Der Auftragnehmer lädt sodann die einzuladende Person unter Nutzung der angegebenen E-Mail Adresse im Auftrag des Auftraggebers zur Nutzung des OOS ein. Auf die gleiche Weise kann der benannte Ansprechpartner weitere Personen in die Funktion eines weiteren Ansprechpartners zur Messeteilnahmeorganisation (ohne Zugriff auf das OOS) einladen lassen.

(bb) Regelmäßig verarbeitete Datenarten: Vorname, Name, Geschlecht, E-Mail Adresse, berufliche Position, Telefon- und Faxnummer.

(cc) Kategorien betroffener Personen: Daten von Ausstellern einschließlich deren Mitarbeitern, Organen und sonstigen Beauftragten sowie Mitarbeitern, Organen und sonstigen Beauftragten der an der Messebeteiligung des Auftraggebers in sonstiger Weise (bspw. in den Bereichen

Presse, Auf- und Abbausteuerung, Technik, Standbau, Standsteuerung während der Laufzeit, Internet und Marketing) beteiligten Unternehmen.

§ 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. 3 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 seiner / seines 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 Auftraggeber dem Auftragnehmer die Kontaktdaten seiner / seines betrieblichen Datenschutzbeauftragten in Textform mit. Die Kontaktdaten der / des betrieblichen Datenschutzbeauftragten des Auftragnehmers sind zudem auf dessen Internetseite 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 im Anhang 1 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 Auftragnehmer bekannt.

(a) für das Matchmaking:

- Intros.at Ltd., 82 Rivington Street, Unit 5, 2nd Floor, EC2A 3AZ, London, England
- Dimedis GmbH, Dillenburger Str. 83, 51105 Köln, Deutschland

(b) für die Aussteller Personalerfassung:

- Dimedis GmbH, Dillenburger Str. 83, 51105 Köln, Deutschland

(c) für die Besucher-Einladungen:

- Dimedis GmbH, Dillenburger Str. 83, 51105 Köln, Deutschland

(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 Abs. 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 Anhang 1 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
Beendigung der Auftragsverarbeitung

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.

ABSCHNITT C – Datenübermittlung in ein Drittland – Standardvertragsklauseln nach 2004/915/EG für die Übermittlung personenbezogener Daten aus der Gemeinschaft in Drittländer (Übermittlung zwischen für die Datenverarbeitung Verantwortlichen)

§ 15
Begriffsbestimmungen

(1) Im Rahmen dieses ABSCHNITT C gelten folgende Begriffsbestimmungen:

(a) Die Begriffe ‚personenbezogene Daten', ‚besondere Kategorien personenbezogener Daten/sensible Daten', ‚verarbeiten/Verarbeitung', ‚für die Verarbeitung Verantwortlicher', ‚Auftragsverarbeiter', ‚betroffene Person' und ‚Kontrollstelle' werden entsprechend den Begriffsbestimmungen der Richtlinie 95/46/EG vom 24. Oktober 1995 verwendet (wobei mit ‚Kontrollstelle' die Datenschutzkontrollstelle gemeint ist, die für das Sitzland des Datenexporteurs zuständig ist).

(b) Datenexporteur' bezeichnet den für die Verarbeitung Verantwortlichen, der die personenbezogenen Daten übermittelt.

(c) ‚Datenimporteur' bezeichnet den für die Verarbeitung Verantwortlichen, der sich bereit erklärt, vom Datenexporteur personenbezogene Daten für die Verarbeitung gemäß den Bestimmungen dieser Vertragsklauseln entgegenzunehmen, und der nicht an ein System eines Drittlandes gebunden ist, das angemessenen Schutz gewährleistet.

(d) ‚Klauseln' bezeichnet diese Standardvertragsklauseln als eigenständiges Dokument, das keine Geschäftsbedingungen beinhaltet, die von den Parteien im Rahmen getrennter geschäftlicher Vereinbarungen getroffen wurden.

(2) Die Einzelheiten der Übermittlung (sowie die abgedeckten personenbezogenen Daten) sind im Folgenden aufgeführt.

(a) Gutscheineinlösung

(i) Betroffene Personen – Die übermittelten personenbezogenen Daten betreffen folgende Kategorien betroffener Personen:

- Messe-Fachbesucher (einschließlich Journalisten) (Repräsentanten von Unternehmen, die Fachmessen besuchen).
- Messe-Besucher (Publikumsveranstaltungen ohne Fachbesucherstatus).
- Clubmitglieder.

(ii) Übermittlungszwecke – Die Übermittlung ist zu folgenden Zwecken erforderlich:

Unternehmer (Datenimporteure), die Besuchergutscheine ausgegeben haben, erhalten die Besucherdaten (Name, Anschrift, Kommunikationsdaten, Kalendertag der Gutscheineinlösung) der eingelösten Gutscheine (zurück-)übermittelt, soweit dies vertraglich vereinbart ist. Dies ermöglicht es den genannten Unternehmern festzustellen, inwieweit die von Ihnen versandten Gutscheine eingelöst wurden.

(iii) Kategorien übermittelter Daten – Die übermittelten personenbezogenen Daten betreffen folgende Datenkategorien:

Bei Messe-Fachbesuchern: Registrierungsdaten wie Firmendaten mit Adressen, Kontaktnamen und Kommunikationsdaten, Kalendertag der Gutscheineinlösung, Branchenzugehörigkeitsinformationen, Produktinteressen sowie Vertrags- und Abrechnungsdaten.

Bei Messe-Besuchern: Name, Anschrift, Kommunikationsdaten, Ausstellerinteressen, Zahlungsdaten, Kalendertag der Gutscheineinlösung.

Bei Clubmitgliedern: Name, Anschrift, Kommunikationsdaten, Ausstellungsinteressen, Zahlungsdaten, persönliche Daten (Geburtsdatum, Haushaltseinkommen, Kaufverhalten, Kalendertag der Gutscheineinlösung)

(iv) Empfänger – Die übermittelten personenbezogenen Daten dürfen nur gegenüber folgenden Empfängern oder Kategorien von Empfängern offengelegt werden:

Keine.

(b) Scan2Lead

(i) Betroffene Personen – Die übermittelten personenbezogenen Daten betreffen folgende Kategorien betroffener Personen:

- Messe-Fachbesucher (einschließlich Journalisten) (Repräsentanten von Unternehmen, die Fachmessen besuchen).
- Clubmitglieder.

(ii) Übermittlungszwecke – die Übermittlung ist zu folgenden Zwecken erforderlich:

Der Datenexporteur bietet Ausstellern (Datenimporteuren) nach gesonderter Bestellung unter dem Namen Scan2Lead den Service einer elektronischen Nutzung der Daten von Fachbesuchern und Clubmitgliedern. Dieser Service besteht unter der Voraussetzung, dass der Besucher als betroffene Person dem Aussteller das Einscannen des auf seiner Eintrittskarte enthaltenen Barcodes gestattet. Der Besucher entscheidet damit selbst, ob seine elektronische "Besucherkarte" zum Aussteller gelangt. Eine Datenübermittlung ist grundsätzlich ausgeschlossen, wenn der Besucher der Weitergabe seiner Daten an den Aussteller widerspricht. Der Aussteller kann mithilfe des Scan2Lead auch nach dem Ende der jeweiligen Messeveranstaltung mit dem Besucher in eigener Verantwortlichkeit in Kontakt treten, um den initial geknüpften Kontakt zu vertiefen.

(iii) Kategorien übermittelter Daten – Die übermittelten personenbezogenen Daten betreffen folgende Datenkategorien:

- Bei Messe-Fachbesuchern: Registrierungsdaten wie Firmendaten mit Adressen, Kontaktnamen und Kommunikationsdaten, Kalendertag der Gutscheineinlösung, Branchenzugehörigkeitsinformationen, Produktinteressen sowie Vertrags- und Abrechnungsdaten.
- Bei Clubmitgliedern: Name, Anschrift, Kommunikationsdaten, Ausstellungsinteressen, Zahlungsdaten, persönliche Daten (Geburtsdatum, Haushaltseinkommen, Kaufverhalten)
- Bei allen Betroffenenkategorien: Zusätze und / oder Änderungen des Datensatzes sowie Notizen, die der Nutzer nach dem Scannen eigenständig dem übertragenen Datensatz im Endgerät und / oder im Scan2Lead-Portal hinzufügt.

(iv) Empfänger – Die übermittelten personenbezogenen Daten dürfen nur gegenüber folgenden Empfängern oder Kategorien von Empfängern offengelegt werden: Keine.

§ 16
Pflichten des Datenexporteurs

Der Datenexporteur gibt folgende Zusicherungen:

(a) Die personenbezogenen Daten wurden nach den für den Datenexporteur geltenden Gesetzen gesammelt, verarbeitet und übermittelt.

(b) Er hat sich im Rahmen des Zumutbaren davon überzeugt, dass der Datenimporteur seine Rechtspflichten aus diesen Klauseln zu erfüllen in der Lage ist.

(c) Er stellt dem Datenimporteur auf Antrag Exemplare der einschlägigen Datenschutzgesetze oder entsprechende Fundstellennachweise seines Sitzlandes zur Verfügung, erteilt aber keine Rechtsberatung.

(d) Er beantwortet Anfragen der betroffenen Personen und der Kontrollstelle bezüglich der Verarbeitung der personenbezogenen Daten durch den Datenimporteur, es sei denn, die Parteien haben vereinbart, dass der Datenimporteur die Beantwortung übernimmt; der Datenexporteur übernimmt die Beantwortung im Rahmen der Zumutbarkeit und aufgrund der ihm zugänglichen Informationen auch dann, wenn der Datenimporteur nicht antworten will oder kann. Sie erfolgt innerhalb einer angemessenen Frist.

(e) Er stellt betroffenen Personen, die Drittbegünstigte im Sinne von § 19 sind, auf Verlangen ein Exemplar der Klauseln zur Verfügung, es sei denn, die Klauseln enthalten vertrauliche Angaben; in diesem Fall hat er das Recht, diese Angaben zu entfernen. Werden Angaben entfernt, teilt der Datenexporteur den betroffenen Personen schriftlich die Gründe für die Entfernung mit und belehrt sie über ihr Recht, die Kontrollstelle auf die Entfernung aufmerksam zu machen. Der Datenexporteur leistet indessen der Entscheidung der Kontrollstelle Folge, den betroffenen Personen Zugang zum Volltext der Klauseln zu gewähren, wenn diese sich zur Geheimhaltung der entfernten vertraulichen Informationen verpflichten. Der Datenexporteur stellt ferner auch der Kontrollstelle auf Antrag ein Exemplar der Klauseln zur Verfügung.

§ 17
Pflichten des Datenimporteurs

Der Datenimporteur gibt folgende Zusicherungen:

(a) Er verfügt über die technischen und organisatorischen Voraussetzungen zum Schutz der personenbezogenen Daten gegen die unbeabsichtigte oder rechtswidrige Zerstörung oder gegen den unbeabsichtigten Verlust oder die unbeabsichtigte Änderung, die unberechtigte Offenlegung oder den unberechtigten Zugriff; damit ist ein Sicherheitsniveau gewährleistet, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten gerecht wird.

(b) Seine Verfahrensregeln gewährleisten, dass von ihm zum Zugriff auf die personenbezogenen Daten befugte Dritte, einschließlich des Auftragsverarbeiters, die Geheimhaltung und Sicherheit der personenbezogenen Daten beachten und wahren. Die unter der Verantwortung des Datenimporteurs tätigen Personen, darunter auch Auftragsverarbeiter, dürfen die personenbezogenen Daten nur auf seine Anweisung verarbeiten. Diese Bestimmung gilt nicht für Personen, die von Rechts wegen zum Zugriff auf die personenbezogenen Daten befugt oder verpflichtet sind.

(c) Zum Zeitpunkt des Vertragsabschlusses bestehen seines Wissens in seinem Land keine entgegenstehenden Rechtsvorschriften, die die Garantien aus diesen Klauseln in gravierender Weise beeinträchtigen; er benachrichtigt den Datenexporteur (der die Benachrichtigung erforderlichenfalls an die Kontrollstelle weiterleitet), wenn er Kenntnis von derartigen Rechtsvorschriften erlangt.

(d) Er verarbeitet die personenbezogenen Daten zu den in § 15 Abs. 2 dargelegten Zwecken und ist ermächtigt, die Zusicherungen zu geben und die Verpflichtungen zu erfüllen, die sich aus diesem Vertrag ergeben.

(e) Er nennt dem Datenexporteur eine Anlaufstelle innerhalb seiner Organisation, die befugt ist, Anfragen bezüglich der Verarbeitung der personenbezogenen Daten zu behandeln, und arbeitet redlich mit dem Datenexporteur, der betroffenen Person und der Kontrollstelle zusammen, damit derartige Anfragen innerhalb einer angemessenen Frist beantwortet werden. Wenn der Datenexporteur nicht mehr besteht oder wenn die Parteien Entsprechendes vereinbaren, verpflichtet sich der Datenimporteur zur Einhaltung der Bestimmungen von § 17 Buchstabe e).

(f) Auf Antrag des Datenexporteurs weist er nach, dass er über ausreichende Finanzmittel verfügt, um die Verpflichtungen aus § 19 zu erfüllen (wozu auch Versicherungsschutz zählen kann).

(g) Auf Antrag des Datenexporteurs und sofern dies nicht willkürlich ist, überlässt er seine zur Verarbeitung benötigten Datenverarbeitungseinrichtungen, Dateien und Unterlagen der Überprüfung, dem Audit und/oder der Zertifizierung durch den Datenexporteur (oder von ihm ausgewählte unabhängige oder unparteiische Prüfer oder Auditoren, gegen die der Datenimporteur keine begründeten Einwände erhebt), um zu gewährleisten, dass die Zusicherungen in diesen Klauseln eingehalten werden, wobei die Überprüfung rechtzeitig anzukündigen und während der üblichen Geschäftszeiten durchzuführen ist. Sofern die Zustimmung oder Genehmigung durch eine Regulierungs- oder Kontrollstelle im Land des Datenimporteurs erforderlich ist, bemüht sich dieser, die Zustimmung oder Genehmigung zügig zu erhalten.

(h) Er verarbeitet die personenbezogenen Daten nach seiner Wahl entweder gemäß

  (i) den Datenschutzbestimmungen des Landes, in dem der Datenexporteur ansässig ist, oder

  (ii) den einschlägigen Bestimmungen (1) etwaiger Kommissionsentscheidungen nach Artikel 25 Abs. 6 der Richtlinie 95/46/EG, sofern der Datenimporteur die einschlägigen Bestimmungen derartiger Genehmigungen bzw. Entscheidungen einhält und in einem Land ansässig ist, für das diese Genehmigungen oder Entscheidungen gelten, obwohl diese hinsichtlich der Übermittlung personenbezogener Daten auf ihn keine Anwendung finden (2), oder

  (iii) den Grundsätzen für die Datenverarbeitung in Anhang 2.

(i) Er verzichtet auf die Offenlegung oder Übermittlung personenbezogener Daten an für die Verarbeitung Verantwortliche Dritte, die außerhalb des Europäischen Wirtschaftsraums (EWR) ansässig sind, es sei denn, er setzt den Datenexporteur von der Übermittlung in Kenntnis und

  (i) der für die Verarbeitung Verantwortliche Dritte verarbeitet die personenbezogenen Daten im Einklang mit einer Kommissionsentscheidung, in der die Kommission einem Drittland ein angemessenes Datenschutzniveau zuerkennt, oder

  (ii) der für die Verarbeitung Verantwortliche Dritte unterzeichnet diese Klauseln oder eine andere, von einer zuständigen Stelle in der EU genehmigte Datenübermittlungsvereinbarung oder

  (iii) die betroffenen Personen haben das Recht zum Widerspruch, nachdem sie über den Zweck der Übermittlung informiert wurden, ferner über die Empfängerkategorien und darüber, dass das Empfängerland der Daten möglicherweise andere Datenschutzstandards aufweist, oder

  (iv) die betroffenen Personen haben im Hinblick auf die Weiterübermittlung sensibler Daten zweifelsfrei ihre Zustimmung zu der Weiterübermittlung erteilt.

§ 18
Haftung und Rechte Dritter

(a) Jede Partei haftet gegenüber der anderen Partei für Schäden, die sie durch einen Verstoß gegen diese Klauseln verursacht. Die gegenseitige Haftung der Parteien ist auf den tatsächlich erlittenen Schaden begrenzt. Strafschadenersatzansprüche (d. h. die Zahlung von Strafen für grobes Fehlverhalten einer Partei)

sind ausdrücklich ausgeschlossen. Jede Partei haftet gegenüber der betroffenen Person für Schäden, die sie durch die Verletzung von Rechten Dritter im Rahmen dieser Klauseln verursacht. Die Haftung des Datenexporteurs gemäß den für ihn maßgeblichen Datenschutzvorschriften bleibt davon unberührt.

(b) Die Parteien räumen den betroffenen Personen das Recht ein, diese Klausel sowie § 16 Buchstaben b), d) und e), § 17 Buchstaben a), c), d), e), h), i), § 18 Buchstabe a) sowie die § 21, § 22 Buchstabe d) und § 23 als Drittbegünstigte gegenüber dem Datenimporteur oder dem Datenexporteur durchzusetzen, wenn diese im Hinblick auf die Daten der betroffenen Personen ihre Vertragspflichten verletzen; zu diesem Zweck erkennen sie die Zuständigkeit der Gerichte im Sitzland des Datenexporteurs an. Wirft die betroffene Person dem Datenimporteur Vertragsverletzung vor, muss sie den Datenexporteur zunächst auffordern, ihre Rechte gegenüber dem Datenimporteur durchzusetzen; wird der Datenexporteur nicht innerhalb einer angemessenen Frist tätig (im Regelfall innerhalb eines Monats), kann die betroffene Person ihre Rechte direkt gegenüber dem Datenimporteur durchsetzen. Eine betroffene Person kann direkt gegen einen Datenexporteur vorgehen, wenn dieser sich im Rahmen des Zumutbaren nicht davon überzeugt hat, dass der Datenimporteur seine rechtlichen Verpflichtungen aus diesen Klauseln zu erfüllen in der Lage ist (der Datenexporteur muss beweisen, dass er alle zumutbaren Anstrengungen unternommen hat).

§ 19
Anwendbares Recht

Diese Klauseln unterliegen dem Recht des Landes, in dem der Datenexporteur ansässig ist; davon ausgenommen sind die Rechtsvorschriften über die Verarbeitung der personenbezogenen Daten durch den Datenimporteur gemäß § 18 Buchstabe h), die nur gelten, wenn sich der Datenimporteur nach dieser Klausel dafür entschieden hat.

§ 20
Beilegung von Streitigkeiten mit betroffenen Personen oder der Kontrollstelle

(a) Bei einer Streitigkeit oder einer Klage der betroffenen Person oder der Kontrollstelle gegen eine Partei oder beide Parteien bezüglich der Verarbeitung personenbezogener Daten setzen die Parteien einander davon in Kenntnis und bemühen sich gemeinsam um eine zügige, gütliche Beilegung.

(b) Die Parteien erklären sich bereit, sich jedem allgemein zugänglichen, nicht bindenden Schlichtungsverfahren zu unterwerfen, das von einer betroffenen Person oder der Kontrollstelle angestrengt wird. Beteiligen sie sich an dem Verfahren, können sie dies auf dem Weg der Telekommunikation tun (z. B. per Telefon oder anderer elektronischer Mittel). Die Parteien erklären sich ferner bereit, eine Beteiligung an anderen Vermittlungsverfahren, Schiedsverfahren oder sonstigen Verfahren der Streitbeilegung zu erwägen, die für die Zwecke des Datenschutzes entwickelt werden.

(c) Die Parteien unterwerfen sich den rechtskräftigen Endentscheidungen des zuständigen Gerichts im Sitzland des Datenexporteurs oder der Kontrollstelle.

§ 21
Beendigung des Vertrags

(a) Verstößt der Datenimporteur gegen seine Verpflichtungen aus diesen Klauseln, kann der Datenexporteur die Übermittlung personenbezogener Daten an den Datenimporteur vorläufig aussetzen, bis der Verstoß beseitigt oder der Vertrag beendet ist.

(b) Tritt einer der folgenden Fälle ein:

(i) Die Übermittlung personenbezogener Daten an den Datenimporteur wird vom Datenexporteur gemäß Buchstabe a) länger als einen Monat ausgesetzt;

(ii) die Einhaltung dieser Klauseln durch den Datenimporteur verstößt gegen Rechtsvorschriften des Importlandes;

(iii) der Datenimporteur missachtet Zusicherungen, die er im Rahmen dieser Klauseln gegeben hat, in erheblichem Umfang oder fortdauernd;

(iv) das zuständige Gericht im Sitzland des Datenexporteurs oder der Kontrollstelle stellt rechtskräftig fest, dass der Datenimporteur oder der Datenexporteur gegen die Klauseln verstoßen haben, oder

(v) es wird ein Antrag auf Insolvenzverwaltung oder Abwicklung des Datenimporteurs in dessen privater oder geschäftlicher Eigenschaft gestellt, der nicht innerhalb der nach geltendem Recht vorgesehenen Frist abgewiesen wird; die Abwicklung wird gerichtlich angeordnet; für einen beliebigen Teil seines Vermögens wird ein Zwangsverwalter bestellt; ein Treuhänder wird bestellt, falls es sich bei dem Datenimporteur um eine Privatperson handelt; dieser leitet einen außergerichtlichen Vergleich ein, oder es kommt zu einem je nach Rechtsordnung gleichwertigen Verfahren,

so ist der Datenexporteur berechtigt, unbeschadet etwaiger sonstiger Ansprüche gegen den Datenimporteur, diesen Vertrag zu kündigen, wovon er gegebenenfalls die Kontrollstelle in Kenntnis setzt. Tritt einer der in Ziffer i), ii) oder iv) genannten Fälle ein, kann der Datenimporteur seinerseits den Vertrag kündigen.

(c) Jede Partei kann den Vertrag kündigen, wenn i) die Kommission eine positive Angemessenheitsfeststellung gemäß Artikel 25 Abs. 6 der Richtlinie 95/46/EG (oder einer Vorschrift, die diese Vorschrift ersetzt) in Bezug auf das Land (oder einen Bereich davon) trifft, in das die Daten übermittelt und in dem sie vom Datenimporteur verarbeitet werden, oder ii) die Richtlinie 95/46/EG (oder eine Vorschrift, die diese Vorschrift ersetzt) in dem betreffenden Landes unmittelbar zur Anwendung gelangt.

(d) Die Parteien vereinbaren, dass sie auch nach der Beendigung dieses Vertrags, ungeachtet des Zeitpunkts, der Umstände oder der Gründe (ausgenommen die Kündigung gemäß § 22 Buchstabe c), weiterhin an die Verpflichtungen und/oder Bestimmungen dieser Klauseln in Bezug auf die Verarbeitung der übermittelten Daten gebunden sind.

§ 22
Änderung der Klauseln

Die Parteien dürfen diese Klauseln nur zum Zwecke der Aktualisierung von § 15 Abs. 2 ändern; gegebenenfalls müssen sie die Kontrollstelle davon in Kenntnis setzen. Es steht den Parteien allerdings frei, erforderlichenfalls weitere Geschäftsklauseln hinzuzufügen.

§ 23
Beschreibung der Übermittlung

Die Einzelheiten zur Übermittlung und zu den personenbezogenen Daten sind in § 15 Abs. 2 aufgeführt. Die Parteien vereinbaren, dass sie gegebenenfalls in § 15 Abs. 2 enthaltene vertrauliche Informationen nicht gegenüber Dritten offenlegen, es sei denn, sie sind gesetzlich dazu verpflichtet oder handeln auf Aufforderung einer zuständigen Regulierungsstelle oder staatlichen Einrichtung oder gemäß § 16 Buchstabe e). Die Parteien können weitere Anhänge vereinbaren, die zusätzliche Übermittlungen betreffen; diese sind gegebenenfalls der Kontrollstelle zu unterbreiten. Ersatzweise kann § 15 Abs. 2 so formuliert werden, dass er eine Vielzahl von Übermittlungen abdeckt.

ANHANG 1

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	Bestellung eines internen betrieblichen Datenschutzbeauftragter (DSB)

Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (Intranet)	
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

ANHANG 2

Grundsätze für die Datenverarbeitung

1. Zweckbindung: Personenbezogene Daten dürfen nur für die in § 15 Abs. 2 festgelegten oder anschließend von der betroffenen Person genehmigten Zwecke verarbeitet und danach verwendet oder weiter übermittelt werden.

2. Datenqualität und Verhältnismäßigkeit: Personenbezogene Daten müssen sachlich richtig sein und nötigenfalls auf dem neuesten Stand gehalten werden. Sie müssen den Übermittlungs- und Verarbeitungszwecken angemessen und dafür erheblich sein und dürfen nicht über das erforderliche Maß hinausgehen.

3. Transparenz: Die betroffenen Personen müssen Informationen erhalten, die eine Verarbeitung nach Treu und Glauben gewährleisten (beispielsweise Angaben zum Verarbeitungszweck und zur Übermittlung), sofern diese Informationen nicht bereits vom Datenexporteur erteilt wurden.

4. Sicherheit und Geheimhaltung: Der für die Verarbeitung Verantwortliche muss geeignete technische und organisatorische Sicherheitsvorkehrungen gegen die Risiken der Verarbeitung treffen, beispielsweise gegen die unbeabsichtigte oder rechtswidrige Zerstörung oder gegen den unbeabsichtigten Verlust oder die unbeabsichtigte Änderung, die unberechtigte Offenlegung oder den unberechtigten Zugriff. Alle unter der Verantwortung des für die Verarbeitung Verantwortlichen tätigen Personen, darunter auch Auftragsverarbeiter, dürfen die Daten nur auf Anweisung des für die Verarbeitung Verantwortlichen verarbeiten.

5. Recht auf Auskunft, Berichtigung, Löschung und Widerspruch: Nach Artikel 12 der Richtlinie 95/46/EG hat die betroffene Person das Recht, entweder direkt oder durch Dritte, Auskunft über alle ihre personenbezogenen Daten zu erhalten, die von einer Organisation vorgehalten werden; dies gilt nicht für Auskunftsersuchen, die aufgrund ihrer unzumutbaren Periodizität oder ihrer Zahl, Wiederholung oder Systematik offensichtlich übertrieben sind, oder für Daten, über die nach dem für den Datenexporteur geltenden Recht keine Auskunft erteilt werden muss. Vorbehaltlich der vorherigen Genehmigung durch die Kontrollstelle muss auch dann keine Auskunft erteilt werden, wenn die Interessen des Datenimporteurs oder anderer Organisationen, die mit dem Datenimporteur in Geschäftsverkehr stehen, dadurch ernsthaft geschädigt würden und die Grundrechte und Grundfreiheiten der betroffenen Personen hierdurch nicht beeinträchtigt werden. Die Quellen der personenbezogenen Daten müssen nicht angegeben werden, wenn dazu unzumutbare Anstrengungen erforderlich wären oder die Rechte Dritter dadurch verletzt würden. Die betroffene Person muss das Recht haben, ihre personenbezogenen Daten berichtigen, ändern oder löschen zu lassen, wenn diese unzutreffend sind oder entgegen den vorliegenden Grundsätzen verarbeitet wurden. Bei begründeten Zweifeln an der Rechtmäßigkeit des Ersuchens kann die Organisation weitere Belege verlangen, bevor die Berichtigung, Änderung oder Löschung erfolgt. Dritte, gegenüber denen die Daten offengelegt wurden, müssen von der Berichtigung, Änderung oder Löschung nicht in Kenntnis gesetzt werden, wenn dies mit einem unverhältnismäßigen Aufwand verbunden wäre. Die betroffene Person muss auch aus zwingenden legitimen Gründen, die mit ihrer persönlichen Situation zusammenhängen, Widerspruch gegen die Verarbeitung ihrer personenbezogenen Daten einlegen können. Die Beweislast liegt im Fall einer Ablehnung beim Datenimporteur; die betroffene Person kann eine Ablehnung jederzeit vor der Kontrollstelle anfechten.

6. Sensible Daten: Der Datenimporteur trifft die zusätzliche Vorkehrungen (beispielsweise sicherheitsbezogener Art), die entsprechend seinen Verpflichtungen nach § 17 zum Schutz sensibler Daten erforderlich sind.

7. Direktmarketing: Werden Daten zum Zwecke des Direktmarketings verarbeitet, sind wirksame Verfahren vorzusehen, damit die betroffene Person sich jederzeit gegen die Verwendung ihrer Daten für derartige Zwecke entscheiden kann (‚Opt-out').

8. Automatisierte Entscheidungen: ‚Automatisierte Entscheidungen' im Sinne dieser Klauseln sind mit Rechtsfolgen behaftete Entscheidungen des Datenexporteurs oder des Datenimporteurs bezüglich einer betroffenen Person, die allein auf der automatisierten Verarbeitung personenbezogener Daten zum Zwecke der

Bewertung einzelner Aspekte ihrer Person beruhen, beispielsweise ihrer beruflichen Leistungsfähigkeit, ihrer Kreditwürdigkeit, ihrer Zuverlässigkeit oder ihres Verhaltens. Der Datenimporteur darf keine automatisierten Entscheidungen über eine betroffene Person fällen, es sei denn:

a) i) Der Datenimporteur fällt die Entscheidungen im Rahmen eines Vertragsabschlusses oder der Ausführung eines Vertrags mit der betroffenen Person, und

ii) die betroffene Person erhält die Möglichkeit, die Ergebnisse einer einschlägigen automatisierten Entscheidung mit einem Vertreter der entscheidungtreffenden Partei zu erörtern, oder aber Erklärungen gegenüber dieser Partei abzugeben,

oder

b) die für den Datenexporteur geltenden Rechtsvorschriften sehen etwas anderes vor.