§ 1 Vertragsgegenstand und Dauer des Auftrags

(1) Die m:con – mannheim:congress GmbH, Rosengartenplatz 2, 68161 Mannheim, vertreten durch den Geschäftsführer Herrn Bastian Fiedler (nachstehend m:con, Auftragsverarbeiter bzw. Auftragnehmer genannt) ist auf Grundlage eines separaten Vertrages (nachfolgend „Hauptvertrag“) für ihren Vertragspartner (nachfolgend Kunde bzw. Verantwortlicher oder Auftraggeber genannt) – mit der Erfüllung von Leistungen beauftragt worden. Im Rahmen der Leistungserbringung für den Hauptvertrag kann es zur Verarbeitung von personenbezogenen Daten der m:con für ihren Kunden kommen.

(2) Diese Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz und konkretisieren die Einzelheiten zum Hauptvertrag.

(3) Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei welcher Beschäftigte des Auftragnehmers oder durch den Auftragnehmer beauftragte weitere Auftragsverarbeiter (nachfolgend „Subunternehmer“) personenbezogene Daten des Auftraggebers verarbeiten.

(4) Die Laufzeit und Kündigung dieser Vereinbarung richten sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrages. Eine Kündigung des Hauptvertrages bewirkt automatisch auch eine Kündigung dieses Vertrages. Eine isolierte Kündigung der vorliegenden Vereinbarung ist ausgeschlossen.

§ 2 Konkretisierung des Auftragsinhalts

(1) Der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung und Nutzung der Daten ergeben sich aus dem Hauptvertrag, den Vorgaben dieses Vertrages sowie den auf Grundlage der beiden Verträge erteilten Weisungen des Auftraggebers.

(2) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers.

(3) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

(4) Gegenstand der Verarbeitung personenbezogener Daten können folgende Datenarten/-kategorien sein:

- [x] Kommunikationsdaten (z.B. Telefon, E-Mail)
- [x] Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- [x] Kundenhistorie
- [x] Vertragsabrechnungs- und Zahlungsdaten
- [x] Personenstammdaten (z.B. Personalkennzahlen, Berufsgruppe, Abteilung)
- [x] Mitgliedsdaten (z.B. Daten über etwaige Mitgliedschaften in Vereinigungen, Verbänden)
- [x] Ermäßigungsberechtigungsdaten (z.B. Studenten, Pflegeberufe, Rentner, Gutscheine)
- [x] Kommunikationsdaten, Passdaten, Reisedaten, Hoteldaten.

(5) Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- [x] Beschäftigte des Auftraggebers
- [x] Kunden des Auftraggebers
- [x] Ansprechpartner des Auftraggebers
- [ ] sonstige: auszufüllen

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers gem. § 2 (1) dieser Vereinbarung.

(2) Der Auftragsverarbeiter darf die Auftraggeber-Daten im Rahmen des datenschutzrechtlich Zulässigen für eigene Zwecke auf eigene Verantwortung verarbeiten und nutzen, wenn eine gesetzliche Erlaubnisvorschrift oder eine Einwilligungserklärung des Betroffenen dies gestattet. Auf solche Datenverarbeitungen findet diese Vereinbarung keine Anwendung. In jedem Fall darf der Auftragnehmer die Auftraggeber-Daten anonymisieren und in anonymisierter Form für eigene Zwecke verarbeiten und nutzen.

(3) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu überprüfen. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.
Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

(4) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c DS-GVO, Art. 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1 und Abs. 2 DS-GVO herzustellen. 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 Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind 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 im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen.

(5) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(6) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Daten-Portabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

§ 4 Pflichten und Kontrollrechte des Auftraggebers

(1) Der Auftraggeber ist im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Bestimmungen des Datenschutzgesetzes insbesondere für die Rechtsmäßigkeit der Vergabe der Datenverarbeitung an den Auftragnehmer sowie die Rechtmäßigkeit der Datenverarbeitung verantwortlich.

(2) 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.

(3) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers 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.

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

§ 5 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

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) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt der unter datenschutz@mcon-mannheim.de kontaktierbar ist. Diese Kontaktdaten werden zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

b) Diese Kontaktdaten werden zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

c) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, Art. 29, Art. 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

d) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, Art. 32 DS-GVO, vgl. **Anlage 2**.

e) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

f) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

g) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

h) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

i) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach § 7 dieses Vertrages.

§ 6 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, die 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 darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

(3) Der Auftraggeber stimmt der Beauftragung weiterer Unterauftragnehmer unter dem Vorbehalt zu, dass die in diesem Vertrag genannten Bestimmungen als Mindeststandard zum Datenschutz eingehalten werden.

§ 7 Mitteilung bei Verstößen und Unterstützung

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen 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 Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen,

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung,

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

(2) Im Falle einer Inanspruchnahme einer Vertragspartei durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichtet sich die in Anspruch genommene Vertragspartei die andere Vertragspartei unverzüglich zu informieren. Die Vertragsparteien verpflichten sich bei der Abwehr des Anspruchs gegenseitig zu unterstützen.

(3) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

§ 8 Weisungsbefugnis des Auftraggebers

(1) Weisungen werden durch diesen Vertrag festgelegt und können vom Auftraggeber an die vom Auftragnehmer zu bezeichnete Stelle durch einzelne Weisungen geändert,

ergänzt oder ersetzt werden (sog. Einzelanweisungen), wobei Einzelanweisungen unverzüglich vom Auftraggeber in Textform festzuhalten sind. Änderungen des Verarbeitungsgegenstandes gem. § 2 (2) dieser Vereinbarung bedürfen einer vorherigen gemeinsamen Abstimmung, die entsprechend § 8 (1) S.1 dieser Vereinbarung in Textform festzuhalten ist.

(2) 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.

(3) Auftraggeber und Auftragnehmer verpflichten sich gegenseitig Änderungen (Wechsel oder langfristige Verhinderungen) der Ansprechpartner unverzüglich mitzuteilen.

§ 9 Löschung und Rückgabe von personenbezogenen Daten

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

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

§ 10 Kundenmanagementsystem

Die m:con setzt eine Kundenmanagementsoftware ein und verarbeitet darin Daten, die aus der Vertragserfüllung gewonnenen wurden, die auch Personenbezug haben können, zu den Zwecken (i) der besseren Pflege der Kunden- bzw. Geschäftsbeziehungen, (ii) der Dokumentation (iii), des Reklamations- und Qualitätsmanagements (iv) sowie aus Gründen der Direktwerbung, um Ihnen Informationen und Angebote über Veranstaltungen zuzusenden, die von der m:con durchgeführt werden.
Zu diesen Daten zählen u.a. Name des Ansprechpartners, Kontaktdaten, Position oder Abteilung.
Rechtsgrundlagen dieser Verarbeitung sind, Artikel 6 (1), a, b, f der Europäischen Datenschutzgrundverordnung. Die Verarbeitung erfolgt dabei stets bezogen auf die konkret dargestellten Zwecke.

§ 11 Informationspflichten, Schriftformklausel, Rechtswahl

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang tätigen Dritten unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als „verantwortliche Stelle“ im Sinne der DS-GVO liegen.

(2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragnehmers- bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingung handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

(4) Es gilt deutsches Recht.

[Stand vom 015.07.2020]

Begriffsbestimmungen

- „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.
- „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten, wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.
- Zweck im Sinne dieser Anlage: Umfang, Art, Zweck der Erhebung, Verarbeitung, Nutzung von Daten
- Teilnehmer im Sinne dieser Anlage umfasst Personen, die an der Veranstaltung als Fachbesucher teilnehmen können. Dies können Teilnehmer am Kongress (Ärzte, Fachpersonal), Referenten, Kongresspräsidenten, wissenschaftliche Mitarbeiter, Studenten, Pflegekräfte oder sonstige Personen sein.
- Daten im Sinne dieser Anlagen können sein:
    - Kommunikationsdaten (z.B. Titel, Ansprache, Name, Vorname; Anschrift; Telekommunikationsdaten Telefon, E-Mail);
    - Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse);
    - Kundenhistorie;
    - Vertragsabrechnungs- und Zahlungsdaten (z.B. Zahlungsart);
    - Personenstammdaten (z.B. Personalkennzahlen, Berufsgruppe, Abteilung); Mitgliedsdaten (z.B. Daten über etwaige Mitgliedschaften in Vereinigungen, Verbänden);
    - Ermäßigungsberechtigungsdaten (z.B. Studenten, Pflegeberufe, Rentner, Gutscheine);
    - Planungs- und Steuerungsdaten (z.B. Bearbeitungsstatus, die Freigabe und zu erledigende Aufgaben);
    - Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
    - sonstige Daten (Passdaten, Visumsdaten, Hoteldaten, Diäten, Sprache).

Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag gem. Art. 28 DS-GVO

Anlage 2 – Technisch-organisatorische Maßnahmen – m:con

Technische und organisatorische Maßnahmen (TOM) i.S.d. Art. 32 DSGVO

A. Vorwort

Dieses Dokument beschreibt für Verantwortliche (Auftraggeber) die technisch organisatorischen Maßnahmen für Auftragsverarbeitungsvorgänge der m:con mannheim -congress GmbH, Rosengartenplatz 2, 68163 Mannheim als Auftragsverarbeiter (Auftragnehmer/m:con).

1. Geltungsbereich

Geltungsbereich ist der Standort Mannheim.

2. Dokumentenhistorie

Änderungshistorie

2.0	**Geschäftsführerwechsel**

B. Datenschutz- und Datensicherheitskonzept

Auftraggeber sind angehalten nur dann mit Auftragsverarbeitern zusammenzuarbeiten, wenn diese hinreichende Garantien für Verarbeitung personenbezogener Daten bieten.

Diese Garantien müssen angemessen sein für die konkrete Datenverarbeitung und müssen gewährleisten, dass geeignete technische und organisatorische Maßnahmen getroffen sind, die die Verarbeitung von personenbezogenen im Einklang mit den Anforderungen der EU-DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet wird.

Zu schützende Prinzipien sind hierbei insbesondere die

- Vertraulichkeit:
  Daten, Informationen und Programme sind vor unberechtigten Zugriffen und unbefugter Preisgabe zu schützen.
- Integrität:
  Der Begriff Integrität bezieht sich auf die Korrektheit der verarbeiteten Informationen und Daten.
- Verfügbarkeit:
  Der Begriff der Verfügbarkeit bezieht sich auf Informationen, Daten, Applikationen sowie Systeme und betrifft deren Funktionsfähigkeit bzw. Abrufbarkeit.
- Belastbarkeit:
  Die Belastbarkeit stellt als besonderen Aspekt der Verfügbarkeit die Anforderung, dass Systeme auch im Störfall, Fehlerfall oder bei hoher Belastung möglichst widerstandsfähig ausgestaltet sein müssen.

Im Folgenden werden die technischen organisatorischen Maßnahmen zur Veranschaulichung des angemessenen Schutzniveaus bei der m:con wiedergegeben.

C. Vertraulichkeit gem. Art. 32 Abs. 1 lit. DSGVO

1. Zutrittskontrolle

Die m:con setzt folgende Maßnahmen ein, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.[1]

Technische Maßnahmen	**Organisatorische Maßnahmen**
☒ Alarmanlage an den Gebäudeeingängen	☐ Schlüsselregelung / Liste
☒ Chipkarten / Transpondersysteme	☒ Pförtner
☒ Regelung zur Nutzung der Chips	☒ Mitarbeiter- / Besucherausweise
☒ Videoüberwachung der Eingänge	☒ Besucher dürfen nur in Begleitung mit Mitarbeiter in den Verwaltungstrakt
	☒ Sorgfalt bei Auswahl des Wachpersonals
	☒ Sorgfalt bei Auswahl Reinigungsdienste
	☒ Anweisung zum Verschließen der Büros beim Verlassen
	☒ bei Veranstaltungen positionieren von Einlasspersonal bei öffentlichen Veranstaltungen
	☒ Zutrittsregelung für Personengruppen (Mitarbeiter, Führungskräfte, Firmenfremde, Besucher, Dienstleister, Lieferanten, Boten)

2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.[2]

1 *Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z.B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.*

2 *Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte*

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Login mit Benutzername + Passwort	☒ Verwalten von Benutzerberechtigungen
☒ getrennter Internetzugriff für Besucher und Mitarbeiter	☒ Regelungen für die Vergabe und Verwaltung von Zugangsberechtigungen
☒ Single Sign-On in Teilbereichen	☒ Regeln beim internen Arbeitsplatzwechsel und Ausscheiden von Mitarbeitern
☒ Sperren des Accounts beim 3-maligem Fehlversuch der Anmeldung	☒ Regeln zu Passwortaktualisierung und Vergabe
☒ Automatische Desktopsperre bei Abwesenheit	☒ Erstellen von Benutzerprofilen
☒ Anti-Viren-Software Server	☒ Zentrale Passwortvergabe
☒ Anti-Virus-Software Clients	☒ Allg. Richtlinie Datenschutz und / oder Sicherheit
☒ Firewall	☒ Handlungsanweisung „Clean desk“

3. Zugriffskontrolle/ Benutzerkontrolle

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.[3]

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Aktenschredder (Stufe 4)	☒ Einsatz Berechtigungskonzepte
☒ teilweiser Nachweis der Benutzung von Datenverarbeitungssystemen (Protokollierung)	☒ Physische Löschung von Datenträgern durch zertifizierte Unternehmen
☒ Protokollierung der Vergabe / Änderung von Zugangsberechtigungen	☒ Verwaltung Benutzerrechte durch Administratoren
☒ Sperrung nach mehrmaligen fehlerhafter Passwortangabe	

Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z.B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten“ Passworts).

3 *Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z.B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.*

4. 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 Test-umgebung	☒ Steuerung über Berechtigungskonzept
☒ Mandantenfähigkeit relevanter Anwendungen	☐ Datensätze sind mit Zweckattributen er-sehen
☒ Zugriffsberechtigungen nach funktioneller Zuständigkeit	

5. Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

Technische Maßnahmen	Organisatorische Maßnahmen
Werden vom Auftragnehmer nur weisungsgebunden im Einzelfall realisiert	

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

1. Weitergabekontrolle[4]

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Einsatz von VPN	☐ Dokumentation der Datenempfänger sowie der Dauer der geplanten Über-lassung bzw. der Löschfristen
☒ Bereitstellung über verschlüsselte Verbindungen wie sftp, https	☐ Regeln zum Umgang mit mobilen Speichermedien (Laptop, Mobiltelefon)
	☒ Regelungen zum Versenden von größeren Dateienmengen über One-Drive

2. 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. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

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
	☒ 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

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

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.[5]

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Feuer- und Rauchmeldeanlagen	
☒ Brandlastreduzierung wird geachtet	☒ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
☒ Feuerlöscher im Serverraum	
☒ Serverraum klimatisiert	☒ Keine sanitären Anschlüsse im oder oberhalb des Serverraums
☒ Wartungsvertrag für Klimaanlage	
☒ Mehrere Klimamodule zur optimalen Kälteverteilung	☒ Getrennte Partitionen für Betriebs-systeme und Daten
☒ USV	
☒ Kontrolle der USV	
☒ RAID System / Festplattenspiegelung	
☒ Videoüberwachung Serverraum	

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

1.1.Datenschutz-Management

Technische Maßnahmen	Organisatorische Maßnahmen

4 *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. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z.B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.*

5 *Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.*

☒ Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz für Mitarbeiter nach Bedarf im Intranet	☒ (Interner) betrieblicher Datenschutz-beauftragter
	☒ Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet
	☒ Regelmäßige Sensibilisierung der Mitarbeiter durch Schulung von Datenschutzkoordinatoren
	☒ Die Datenschutz-Folgenabschätzung wird bei Bedarf durchgeführt
	☒ Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO
	☒ Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden
	☒ Erarbeitung eines Datenschutzhandbuches
	☒ jährliche Überprüfung der Verarbeitungsverzeichnisse

1.2. Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Technische Maßnahmen	**Organisatorische Maßnahmen**
☒ Einsatz von Firewall und regelmäßige Aktualisierung	☒ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen
☒ Einsatz von Spamfilter und regelmäßige Aktualisierung	☒ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
☒ Einsatz von Virenscanner und regelmäßige Aktualisierung	☒ Einbindung von ☒ DSB und ☒ IT Verantwortlichen in Sicherheitsvorfälle und Datenpannen
	☒ Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
	☒ Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

1.3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);

Privacy by design / Privacy by default

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

1.4. Auftragskontrolle (Outsourcing an Dritte)

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. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.

Technische Maßnahmen	**Organisatorische Maßnahmen**
	☒ Vorherige Prüfung der vom Auftrag-nehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
	☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit
	☒ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung
	☒ 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 Kontrollrechte gegenüber dem Auftragnehmer
	☒ Regelung zum Einsatz weiterer Sub-unternehmer
	☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
	☒ Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus

Ort, Datum: 17.01.2020