MD CLOUD SERVICES GmbH

Im Taubental 25
41468 Neuss

Tel: +49 (0) 21 31 - 7 51 98-0
Fax: +49 (0) 21 31 - 7 51 98-99

info@mdcloudservices.de
www.mdcloudservices.de

VERTRAG AUFTRAGSVERARBEITUNG PERSONENBEZOGENER DATEN

ZWISCHEN ANBIETER (IM FOLGENDEN „AUFTRAGSVERARBEITER“)

MD CLOUD SERVICES GmbH
Vertretung durch: Ingo Kalker (Geschäftsführer)
Im Taubental 25
41468 Neuss

UND KUNDE (IM FOLGENDEN „VERANTWORTLICHER“)

Firma

Vertreten durch (Vor- und Nachname)

Straße & Hausnummer

PLZ *Ort*

Tel

qms-vertrag-verarbeitung-personen-bezogener-daten-rev-26-08-2022

MD CLOUD SERVICES GmbH
Sitz der Gesellschaft: Neuss
Handelsregister Neuss HRB-NR. 22400
USt.-ID-Nr. DE 210 900 969

Bank: Commerzbank AG, Neuss
IBAN: DE 11 3004 0000 0752 7500 00
BIC: COBADEFFXXX

Geschäftsführer: Ingo Kalker

MD CLOUD SERVICES

PRÄAMBEL

Die Vertragsparteien sind mit der Leistungsvereinbarung ein Auftragsverarbeitungsverhältnis (im Folgenden „AV-Vertrag“ genannt) eingegangen. Um die sich hieraus ergebenden Rechte und Pflichten gemäß den Vorgaben der europäischen Datenschutz-Grundverordnung (Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG - DSGVO), und des Bundesdatenschutzgesetzes (BDSG) zu konkretisieren, schließen die Vertragsparteien die nachfolgende Vereinbarung.

1. EINLEITUNG, GELTUNGSBEREICH, DEFINITIONEN

1.1. Der AV-Vertrag regelt die Rechte und Pflichten von Auftragsverarbeiter und Verantwortlichem (im Folgenden „Parteien“ genannt) im Rahmen einer Verarbeitung personenbezogener Daten im Auftrag.

1.2. Der AV-Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragsverarbeiters oder durch ihn beauftragte Unterauftragsverarbeiter (Subunternehmer) personenbezogene Daten des Verantwortlichen verarbeiten.

1.3. In diesem AV-Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen. Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Schriftform nach §126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

2. GEGENSTAND UND DAUER DER VERARBEITUNG

2.1. Gegenstand

Das Unternehmen des Auftragsverarbeiters stellt seinen Kunden eine virtuelle Arbeitsumgebung auf einem Server-Cluster oder eigens erstelltem Server zur Verfügung um Software der Konzerngruppe und andere Produkte ortsunabhängig und in sicherer Umgebung zu nutzen. Dabei handelt es sich um die Erbringung von Leistungen der Datenverarbeitung und der Telekommunikation, wie Installation, Konfiguration, Betrieb und Erweiterung der Arbeitsumgebung, sowie zugehörige Dienstleistungen, wie Support, Fernwartung, Datensicherung und Monitoring der Systeme. Die Verarbeitung beruht auf dem zwischen den Parteien bestehenden Geschäftskundenauftrag (im Folgenden „Hauptvertrag“ genannt).

2.2. Dauer

Die Verarbeitung beginnt mit Unterzeichnung des Hauptvertrages und erfolgt auf unbestimmte Zeit bis zur Kündigung des Hauptvertrags durch eine Partei.

3. ART UND ZWECK DER DATENERHEBUNG, -VERARBEITUNG ODER –NUTZUNG

3.1. Art und Zweck der Verarbeitung

Die gesamte Auftragsverarbeitung dient dem Zweck, dem Verantwortlichen eine virtuelle Arbeitsumgebung bereitzustellen in der Software der Konzerngruppe und andere Produkte genutzt werden können. Dabei und im Rahmen des Supports werden personenbezogene Daten verarbeitet, welche inhaltlich für den Auftragsverarbeiter nicht qualifizierbar sind und die insoweit ausschließlich durch den Verantwortlichen bestimmt werden. Der Auftragsverarbeiter ist wie folgt in der Datenverarbeitung einbezogen:

(a) Organisation
(b) Ordnen
(c) Speicherung
(d) Auslesen
(e) Übermitteln
(f) Löschen

Die Verarbeitung der Daten durch den Auftragsverarbeiter erfolgt im Rahmen des AV-Vertrags ausschließlich zum Zwecke der Bereitstellung, Sicherstellung der Verfügbarkeit, Dateisystem- und Datenbankoptimierung, sowie der Entstörung.

MD CLOUD SERVICES GmbH
Sitz der Gesellschaft: Neuss
Handelsregister Neuss HRB-NR. 22400
USt.-ID-Nr. DE 210 900 969

Bank: Commerzbank AG, Neuss
IBAN: DE 11 3004 0000 0752 7500 00
BIC: COBADEFFXXX

Geschäftsführer: Ingo Kalker

3.2. Art der Daten

Die vom Auftragsverarbeiter verarbeiteten Daten umfassen personenbezogene Daten aus den jeweils von dem Verantwortlichen auf der durch den Auftragsverarbeiter zur Verfügung gestellten Plattform („Cloud"). Diese Daten können folgende Kategorien haben:

- Personenstammdaten
- Vertragsstammdaten
- Kundenhistorie
- Vertrags- und Zahlungsdaten
- Planungs- und Steuerungsdaten
- Kommunikationsdaten
- Informationen über Gesundheit, Pflegebedarf und Medikation.

Die Verantwortung für die Art der Daten liegt ausschließlich beim Verantwortlichen. Es obliegt dem Verantwortlichen, den Auftragsverarbeiter ggf. über die Verarbeitung besonders schützenswerter Datenkategorien, wie z.B. personenbezogene Stammdaten, Gesundheitsdaten, Abrechnungsdaten, Gesundheitsdaten, Abrechnungsdaten zu informieren. Es sei denn, die vom Auftragsverarbeiter für den Verantwortlichen zu verwaltende Software kann entsprechende Kategorien verarbeiten und dem Auftragsverarbeiter ist dieses bekannt. In diesem Fall wird eine Verarbeitung der möglichen Datenkategorien vom Auftragsverarbeiter angenommen.

3.3. Kategorien der betroffenen Personen

Nur der Verantwortliche bestimmt über die Art der gespeicherten Daten und die von der Datenverarbeitung betroffenen Personengruppen. Daher kann der Auftragsverarbeiter hierüber keine endgültige Aussage machen. Es sei denn, diese Informationen werden dem Auftragsverarbeiter im Einzelfall konkret benannt.
Aufgrund unserer Erfahrungen mit der auf unseren Systemen gehosteten Anwendersoftware gehen wir davon aus, dass folgende Personen von den beim Auftragsverarbeiter gehosteten Systemen betroffen sind:

- Kunden
- Interessenten
- Mitarbeiter
- Dritte (z.B. Familienangehörige, Betreuer, Ärzte, Versorger, Erziehungsberechtigte, Familienhelfer)

Es liegt im Bereich des Verantwortlichen, den Auftragsverarbeiter zu informieren, wenn weitere Personengruppen als Betroffene identifiziert werden.

4. PFLICHTEN DES AUFTRAGSVERARBEITERS

4.1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Verantwortlichen angewiesen, es sei denn, der Auftragsverarbeiter ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragsverarbeiter diese dem Verantwortlichen vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Auftragsverarbeiter verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

4.2. Der Auftragsverarbeiter bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung. Er hat einen Datenschutzbeauftragen benannt.

4.3. Der Auftragsverarbeiter verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.

4.4. Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.

4.5. Der Auftragsverarbeiter sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und des AV-Vertrags vertraut gemacht wurden und auf die Geheimhaltung etwaiger Privatgeheimnisse nach § 203 StGB verpflichtet sind. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Der Auftragsverarbeiter trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.

4.6. Unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützt der Auftragsverarbeiter bei der Durchführung einer Datenschutzfolgenabschätzung. Alle erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Verantwortlichen auf Anforderung unverzüglich zuzuleiten.

4.7. Wird der Verantwortliche durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragsverarbeiter den Verantwortlichen im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.

MD CLOUD SERVICES GmbH
Sitz der Gesellschaft: Neuss
Handelsregister Neuss HRB-NR. 22400
USt.-ID-Nr. DE 210 900 969

Bank: Commerzbank AG, Neuss
IBAN: DE 11 3004 0000 0752 7500 00
BIC: COBADEFFXXX

Geschäftsführer: Ingo Kalker

4.8. Auskünfte an Dritte oder den Betroffenen darf der Auftragsverarbeiter – vorbehaltlich gesetzlicher Verpflichtungen – nur nach vorheriger Zustimmung durch den Verantwortlichen erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Verantwortlichen weiterleiten.

4.9. Der Auftragsverarbeiter hat eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz benannt. Es ist sichergestellt, dass für den Beauftragten keine Interessenskonflikte bestehen. In Zweifelsfällen kann sich der Verantwortliche direkt an den Datenschutzbeauftragten wenden. Der Auftragsverarbeiter teilt dem Auftraggeber unverzüglich die Kontaktdaten des Datenschutzbeauftragten mit. Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt der Auftragsverarbeiter dem Verantwortlichen unverzüglich mit.

4.10. Die Auftragsverarbeitung erfolgt grundsätzlich innerhalb der EU oder des EWR. Jegliche Verlagerung in ein Drittland darf nur mit Zustimmung des Verantwortlichen und unter den in Kapitel V der Datenschutz-Grundverordnung enthaltenen Bedingungen sowie unter Einhaltung der Bestimmungen des AV-Vertrags erfolgen.

5. TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

5.1. Die im Anlage 1 beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt. Sie definieren das vom Auftragsverarbeiter geschuldete Minimum. Die Beschreibung der Maßnahmen muss so detailliert erfolgen, dass für einen sachkundigen Dritten allein aufgrund der Beschreibung jederzeit zweifelsfrei erkennbar ist, was das geschuldete Minimum sein soll. Ein Verweis auf Informationen, die dieser Vereinbarung oder ihren Anlagen nicht unmittelbar entnommen werden können, ist nicht zulässig.

5.2. Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entspre- chend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat der Auftragsverarbeiter unverzüglich umzusetzen. Änderungen sind dem Verantwortlichen unverzüglich mitzuteilen. Wesentliche Änderungen sind zwischen den Parteien zu vereinbaren.

5.3. Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Verantwortlichen nicht oder nicht mehr genügen, benachrichtigt der Auftragsverarbeiter den Verantwortlichen unverzüglich.

5.4. Der Auftragsverarbeiter sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

5.5. Kopien oder Duplikate werden ohne Wissen des Verantwortlichen nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.

5.6. Die Daten werden grundsätzlich an den Standorten des Auftragsverarbeiters verarbeitet. Soweit eine Verarbeitung an mobilen Arbeitsplätzen erfolgt, ist vom Auftragsverarbeiter sicherzustellen, dass dabei ein diesem AV-Vertrag entsprechendes Niveau an Datenschutz und Datensicherheit aufrechterhalten wird und die in diesem AV-Vertrag bestimmten Kontrollrechte des Verantwortlichen uneingeschränkt auch an den mobilen Arbeitsplätzen ausgeübt werden können.

5.7. Der Auftragsverarbeiter führt den regelmäßigen Nachweis der Erfüllung seiner Pflichten, insbesondere der vollständigen Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen sowie ihrer Wirksamkeit. Den Nachweis wird der Auftragsverarbeiter auf Verlangen des Verantwortlichen erbringen. Der Nachweis kann durch genehmigte Zertifizierungsverfahren erbracht werden.

6. REGELUNGEN ZUR BERICHTIGUNG, LÖSCHUNG UND SPERRUNG VON DATEN

6.1. Im Rahmen des Auftrags verarbeitete Daten wird der Auftragsverarbeiter nur entsprechend der getroffenen vertraglichen Vereinbarungen oder nach Weisung des Verantwortlichen berichtigen, löschen oder sperren.

6.2. Den entsprechenden Weisungen des Verantwortlichen wird der Auftragsverarbeiter jederzeit und auch über die Beendigung dieses AV-Vertrages hinaus Folge leisten.

MD CLOUD SERVICES GmbH
Sitz der Gesellschaft: Neuss
Handelsregister Neuss HRB-NR. 22400
USt.-ID-Nr. DE 210 900 969

Bank: Commerzbank AG, Neuss
IBAN: DE 11 3004 0000 0752 7500 00
BIC: COBADEFFXXX

Geschäftsführer: Ingo Kalker

7. UNTERAUFTRAGSVERHÄLTNISSE

7.1. Die Beauftragung von Subunternehmern ist nur mit schriftlicher Zustimmung des Verantwortlichen im Einzelfall zugelassen.

7.2. Die Zustimmung ist nur möglich, wenn dem Subunternehmer vertraglich mindestens Datenschutzpflichten auferlegt wurden, die den in diesem AV-Vertrag vereinbarten vergleichbar sind. Der Verantwortliche erhält auf Verlangen Einsicht in die relevanten Verträge zwischen Auftragsverarbeiter und Subunternehmer.

7.3. Die Rechte des Verantwortlichen müssen auch gegenüber dem Subunternehmer wirksam ausgeübt werden können. Insbesondere muss der Verantwortliche berechtigt sein, seine Überwachungs- und Kontrollpflichten auch bzgl. der Subunternehmer in gebotenem Umfang wahrzunehmen.

7.4. Die Verantwortlichkeiten des Auftragsverarbeiters und des Subunternehmers sind eindeutig voneinander abzugrenzen.

7.5. Eine weitere Subbeauftragung durch den Subunternehmer ist nicht zulässig.

7.6. Der Auftragsverarbeiter wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus.

7.7. Die Weiterleitung von im Auftrag verarbeiteten Daten an den Subunternehmer ist erst zulässig, wenn sich der Auftragsverarbeiter dokumentiert davon überzeugt hat, dass der Subunternehmer seine Verpflichtungen vollständig erfüllt hat. Der Auftragsverarbeiter hat dem Verantwortlichen die Dokumentation unaufgefordert vorzulegen.

7.8. Die Beauftragung von Subunternehmern, die Verarbeitungen im Auftrag nicht ausschließlich aus dem Gebiet der EU oder des EWR erbringen, erfolgt nur mit Zustimmung des Verantwortlichen und unter den in Kapitel V der Datenschutz-Grundverordnung enthaltenen Bedingungen sowie unter Einhaltung der Bestimmungen dieses AV-Vertrags.

7.9. Der Auftragsverarbeiter hat die Einhaltung der Pflichten des Subunternehmers regelmäßig, spätestens alle 12 Monate, angemessen zu überprüfen. Die Prüfung und ihr Ergebnis sind so aussagekräftig zu dokumentieren, dass sie für einen fachkundigen Dritten nachvollziehbar sind. Die Dokumentation ist dem Verantwortlichen auf Verlangen vorzulegen.

7.10. Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet hierfür der Auftragsverarbeiter gegenüber dem Verantwortlichen.

7.11. Zurzeit sind die in Anlage 2 mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt und durch den Verantwortlichen genehmigt. Die hier niedergelegten sonstigen Pflichten des Auftragsverarbeiters gegenüber Subunternehmern bleiben unberührt.

7.12. Unterauftragsverhältnisse im Sinne dieses AV-Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen, wie beispielsweise Transport, Wartung und Reinigung sowie die Inanspruchnahme von Telekommunikationsdienstleistungen oder Benutzerservice sind nicht erfasst. Die Pflicht des Auftragsverarbeiters, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

8. RECHTE UND PFLICHTEN DES VERANTWORTLICHEN

8.1. Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Be- troffenen ist allein der Verantwortliche zuständig. Sofern erforderlich, unterstützt der Auftragsverarbeiter den Verantwortlichen gem. Art. 36 DSGVO bei der Konsultation von Aufsichtsbehörden.

8.2. Der Verantwortliche erteilt alle Aufträge, Teilaufträge oder Weisungen schriftlich dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Verantwortliche unverzüglich schriftlich dokumentiert bestätigen.

8.3. Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

8.4. Der Verantwortliche ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragsverarbeiter in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragsverarbeiter soweit erforderlich Zutritt und Einblick zu ermöglichen. Der Auftragsverarbeiter ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind.

MD CLOUD SERVICES GmbH
Sitz der Gesellschaft: Neuss
Handelsregister Neuss HRB-NR. 22400
USt.-ID-Nr. DE 210 900 969

Bank: Commerzbank AG, Neuss
IBAN: DE 11 3004 0000 0752 7500 00
BIC: COBADEFFXXX

Geschäftsführer: Ingo Kalker

8.5. Kontrollen beim Auftragsverarbeiter haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Verantwortlichen zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nur nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragsverarbeiters, sowie nicht häufiger als alle 12 Monate statt. Soweit der Auftragsverarbeiter den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten wie unter Kapitel 5.7 dieses AV-Vertrages vorgesehen erbringt, soll sich eine Kontrolle auf Stichproben beschränken.

9. MITTEILUNGSPFLICHTEN

9.1. Der Auftragsverarbeiter teilt dem Verantwortlichen Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung hat spätestens innerhalb von 24 Stunden ab Kenntnis des Auftragsverarbeiters vom relevanten Ereignis an eine vom Verantwortlichen benannte Adresse zu erfolgen. Sie muss mindestens folgende Angaben enthalten:

(a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Ka- tegorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
(b) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
(c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Da- ten;
(d) eine Beschreibung der vom Auftragsverarbeiter ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

9.2. Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße des Auftragsverarbeiters oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem AV-Vertrag getroffenen Festlegungen.

9.3. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.

9.4. Der Auftragsverarbeiter sichert zu, den Verantwortlichen bei dessen Pflichten nach Art. 33 und 34 Datenschutz-Grundverordnung im erforderlichen Umfang zu unterstützen.

10. WEISUNGEN

10.1. Der Verantwortliche behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.

10.2. Verantwortlicher und Auftragsverarbeiter benennen die zur Erteilung und Annahme von Weisungen ausschließlich befugten Personen in Anlage 3.

10.3. Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen sind der anderen Partei Nachfolger bzw. Vertreter unverzüglich mitzuteilen.

10.4. Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich darauf aufmerksam machen, wenn eine vom Verantwortlichen erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftragsverarbeiter bestätigt oder geändert wird.

10.5. Der Auftragsverarbeiter hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.

11. BEENDIGUNG DES AUFTRAGS

11.1. Nach Abschluss der Auftragsverarbeitung hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangten Unterlagen, Datenträger und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen und personenbezogene Daten enthalten, an den Verantwortlichen zurückzugeben. Alle weiteren personenbezogenen Daten vom Verantwortlichen sind unverzüglich zu löschen, es sei denn der Löschung stehen gesetzliche Speicherfristen entgegen.

11.2. Der Auftragsverarbeiter ist verpflichtet, die unverzügliche Rückgabe bzw. Löschung auch bei Subunternehmern herbeizuführen.

11.3. Der Auftragsverarbeiter hat den Nachweis der ordnungsgemäßen Vernichtung zu führen und dem Verantwortlichen unverzüglich vorzulegen.

MD CLOUD SERVICES GmbH
Sitz der Gesellschaft: Neuss
Handelsregister Neuss HRB-NR. 22400
USt.-ID-Nr. DE 210 900 969

Bank: Commerzbank AG, Neuss
IBAN: DE 11 3004 0000 0752 7500 00
BIC: COBADEFFXXX

Geschäftsführer: Ingo Kalker

11.4. Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auf- tragnehmer den jeweiligen Aufbewahrungsfristen entsprechend auch über das Vertragsende des Hauptvertrags hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Verantwortlichen bei Vertragsende übergeben.

12. VERGÜTUNG

12.1. Die Vergütung des Auftragsverarbeiters ist abschließend im Hauptvertrag geregelt. Eine gesonderte Vergütung oder Kostenerstattung im Rahmen des AV-Vertrags erfolgt nicht.

13. HAFTUNG

13.1. Der Auftragsverarbeiter haftet für die ordnungsgemäße Ausführung des Auftrags nach den geltenden gesetzlichen Bestimmungen.

13.2. Für Verschulden seiner Unterauftragsverarbeiter haftet der Auftragsverarbeiter wie für eigenes Verschulden.

14. SONSTIGES

14.1. Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses (Hauptvertrag und AV-Vertrag) erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung der Verträge hinaus vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.

14.2. Sollte Eigentum des Verantwortlichen beim Auftragsverarbeiter durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragsverarbeiter den Verantwortlichen unverzüglich zu verständigen.

14.3. Für Nebenabreden ist die Schriftform erforderlich; dieses gilt auch für die Schriftformklausel selbst.

14.4. Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

14.5. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

15. VERTRAGSABSCHLUSS

	MD CLOUD SERVICES GmbH
Verantwortlicher	*Auftragsverarbeiter*
	41468 Neuss, 30. August 2022
Ort, Datum	*Ort, Datum*
Unterschrift (Kunde)	*Unterschrift (Anbieter)*

MD CLOUD SERVICES GmbH
Sitz der Gesellschaft: Neuss
Handelsregister Neuss HRB-NR. 22400
USt.-ID-Nr. DE 210 900 969

Bank: Commerzbank AG, Neuss
IBAN: DE 11 3004 0000 0752 7500 00
BIC: COBADEFFXXX

Geschäftsführer: Ingo Kalker

MD CLOUD SERVICES GmbH

Im Taubental 25
41468 Neuss

Tel: +49 (0) 21 31 - 7 51 98-0
Fax: +49 (0) 21 31 - 7 51 98-99

info@mdcloudservices.de
www.mdcloudservices.de

Anlage 1 zum AV-Vertrag

TECHNISCHE UND ORGANISATORISCHE DATENSCHUTZMASSNAHMEN

1. VERTRAULICHKEIT GEM. ART. 32 ABS. 1 LIT. DSGVO

1.1. Zutrittskontrolle

Der Zutritt zum Rechenzentrum wird kontrolliert durch:
Eine elektronische/biometrische Zutrittskontrolle. Am Eingang werden in Kombination der elektronische Identifikations- chip und der Fingerabdruck des Besuchers überprüft. Um passieren zu können, muss der Fingerabdruck mit dem auf dem Chip gespeicherten übereinstimmen und der Besucher Zutrittserlaubnis haben, inklusive Zugangsprotokollierung Pförtnerdienst, Besucherprotokoll und –ausweise, Besucher dürfen das Rechenzentrum nur in Begleitung eines Mitarbei- ters betreten zwei brand- und einbruchsresistente Stahltüren, wobei diese separat durch die vorig genannte Zutrittskont- rolle zu passieren sind Sabotagegeschützte Verlegung und Überwachung der Leitungen Besonderer Schutz der Sicher- heitszentrale und ein Sicherheitsdienst vor Ort.

Der Zutritt zu unseren Anlagen wird kontrolliert durch:
ein separates Schließsystem unserer Schränke. Die dazugehörigen Schlüssel sind im Besitz der MD CLOUD SERVICES GmbH und des Betreibers des Rechenzentrums. Zudem sind sämtliche Räumlichkeiten, inklusive die des Eingangsbereichs und die der Anlagenstandorte, mit Videoüberwachungssystemen ausgestattet. Die Auswertung dieses Materials erfolgt bei Bedarf durch den Betreiber des Rechenzentrums.

1.2. Zugangskontrolle

Ein Zugangskontrollsystem inklusive entsprechender Zugangsregelung ist sowohl für den Sicherheitsbereich wie auch für alle Infrastruktur-komponenten (z. B. Verteiler) vorhanden (EN 60389-11). Der Einbruchschutz ist mehrstufig ausgelegt und alle sicherheitskritischen Bereiche sind mittels einer Einbruchmeldeanlage überwacht (EN 50131). Dabei sind die Anlagen ebenfalls mit Notstrom versorgt und über einen gesicherten Übertragungsweg (EN50136 und EN 50518) zu einer ständig besetzten Sicherheitszentrale durchgeschaltet. Die Nutzung von IT-Systemen und Applikationen der MD CLOUD SERVICES GmbH ist erst nach hinreichender Authentifizierung des Nutzers am Domänencontroller der MD CLOUD SERVICES GmbH möglich. Die Authentifizierung erfolgt durch die Verwendung der Kombination Benutzername/Passwort. Die Authentifizierung wird durch die jeweils gültige Passwortrichtlinie geregelt (siehe Zugriffskontrolle). Zum Schutz gegen Schadinhalte wird auf allen Servern und Clients, sofern technisch möglich, eine Antivirensoftware eingesetzt. Insbesondere eingehende E-Mail-Kommunikation wird durch die eingesetzten Virenschutzprogramme überprüft. Für den Fall, dass ein Mitarbeiter eine E-Mail mit einem unbekannten bzw. verdächtigen Dateianhang erhält, ist dieser verpflichtet, sich unverzüglich an die IT-Abteilung zu wenden. Der unbekannte bzw. verdächtige Dateianhang darf erst nach Freigabe durch die IT-Abteilung geöffnet werden. Falls ein Fernzugang erforderlich ist, wird dieser Zugriff ebenfalls authentifiziert und über einen VPN-Tunnel realisiert. Sämtlicher eingehender und ausgehender Datenverkehr wird über eine UTM-Firewall geleitet. Zum Schutz vor möglichen Angriffen wird ein Einbruchserkennungssystem eingesetzt (Intrusion Detection System). Mitarbeiter werden gemäß dem geltenden Berechtigungskonzept zu Sicherheitsgruppen, die den Zugriff auf Daten und Dateien regeln, zugeordnet. Zuständig für Zuordnung zu Sicherheitsgruppen ist die IT-Abteilung. Der Vergabe von Zugriffsberechtigungen auf Daten der Firmendatenbank wird durch die Datenbankadministration gesteuert.

1.3. Zugriffskontrolle

Sämtliche Zugriffe auf Daten und Programme ist dem jeweiligen Mitarbeiter nur gemäß Berechtigungskonzept möglich. Mitarbeiter können ausschließlich auf Ressourcen zugreifen, welche tatsächlich für den Bearbeitungszweck vorgesehen sind. Gewährleistet wird dies durch den vorgenannten Einsatz eines Berechtigungskonzepts. In diesem Konzept wird der Zugriff von Mitarbeiter auf Ressourcen der jeweiligen Fachabteilung definiert. Grundsätzlich verfügt kein Mitarbeiter über vollumfängliche Domänen-Administrationsberechtigungen. Über diese verfügen ausschließlich ein sehr kleiner, über schaubarer Kreis von Mitarbeitern mit entsprechenden technischen und persönlichen Qualifikationen. Die Passwortricht linie des Unternehmens definiert die Mindestlänge, Komplexität, Gültigkeit und Wechsel der von den Mitarbeitern einge- setzten Passwörter. Bei Verlassen des Arbeitsplatzes wird die Benutzersitzung des Mitarbeiters, nach Ablauf einer Leer- laufzeit, automatisch gesperrt. Die Wiederaufnahme setzt eine erneute Authentifizierung voraus. Allen Nutzern werden, bei Beantragung durch weisungsbefugte Personen des Verantwortlichern, ein Benutzernamen sowie ein Passwort zugewiesen. Soweit technisch möglich wird jeder Nutzer gezwungen, sein Initial-Passwort unverzüglich in ein Passwort gemäß der vereinbarten Passwort-Richtlinie zu ändern.

1.4. Trennungsgebot

Daten, welche für unterschiedliche Zwecke bestimmt sind, werden in unterschiedlichen Speicherbereichen gespeichert. So werden Daten, welche durch einen Benutzer in unsere Datenverarbeitungssysteme eingegeben werden, getrennt von anderen Daten, beispielsweise systemverwaltungstechnische Daten, in einem kundenspezifischen Speicherbereich abgelegt. Konkret unterschieden werden benutzergenerierte Dokumente und Dateien, E-Mails, Datenbanken, Programm- code, Datensicherungsarchive und Anmeldeinformationen. Unsere Systeme und Netzwerke sind ihrer Funktion nach auf- geteilt. So ist sichergestellt, dass beispielsweise Datenbankserver ausschließlich Datenbanken bereitstellen und Spei- chernetzwerke ausschließlich zur Kommunikation mit Speichersystemen genutzt werden.

2. INTEGRITÄT (ART. 32 ABS. 1 LIT. B DSGVO)

2.1. Weitergabekontrolle

Die Weitergabe der Daten unserer Datenverarbeitungssysteme wird zum einen durch mechanischen und physikalische Sicherheitseinrichtung (abgeschlossene Serverschränke, Zutrittskontrollen), zum anderen durch softwaretechnische Maßnahmen (Verschlüsselte Datenübertragung zwischen authentifizierten Systemkomponenten und externer kundenei- genen Komponenten, wie der Hardware, welche zum Zugang zu unseren Datenverarbeitungssystemen genutzt wird), kontrolliert. Konkret bedeutet das, dass der Zugriff auf unsere Systeme durch unsere Kunden ausschließlich verschlüsselt erfolgt (bspw. Remote Desktop über HTTPS, Hochladen von Daten über FTPS, Postfachzugriff über eine gesicherte Exchange- / IMAP-Verbindung).

2.2. Eingabekontrolle

Der Zugriff auf Dateien erfolgt, gemäß Berechtigungskonzept, unter Verwendung von individuellen Benutzerkonten. Da bei wird im Allgemeinen zwischen Lese- und Schreibzugriffen unterschieden. Änderungen dieser Berechtigungen oblie- gen dem Administrator. Die Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Be- rechtigungskonzepts werden in der jeweiligen Branchensoftware selbst durch den Verantwortlichen vorgenommen.

3. VERFÜGBARKEIT UND BELASTBARKEIT (ART. 32 ABS. 1 LIT. B DSGVO)

3.1. Verfügbarkeitskontrolle

Das Gebäude umgibt die aufgestellte Informationstechnik und bietet einen äußeren Schutz. Die Lage des Gebäudes spielt hinsichtlich der umliegenden Gefahrenpotenziale ebenso eine Rolle, wie die Lage des Sicherheitsbereichs im Gebäude, um gegebenen potenziellen Gefahrenquellen a priori auszuweichen. Umgebungsgefährdungen, hervorgerufen durch Wasser, Explosionen, Trümmer, Erschütterungen oder Schadstoffe werden gemieden. Ebenso werden Verkehrs- wege mit Gefahrguttransporten gemieden, um sich direkten wie indirekten Auswirkungen, wie z. B. Absperrungen, zu entziehen. Das Mauerwerk, Fenster und Türen bieten einen Zugriffs- (DIN V EN 1627), Brand- und Rauchschutz (DIN 18095). Ebenso ist sichergestellt, dass wassergefährdete Gebäudeabschnitte (VdS 2007), EM/RF-Störfelder (EN 50147 Teil 1) und gefährliche Produktionsprozesse in angrenzenden Räumen gemieden werden. Das Gebäude verfügt über einen äußeren Blitzschutz (EN 62305-1) und mindestens der Sicherheitsbereich stellt einen eigenen Brandabschnitt dar (DIN 4102). Die Versorgungsleitungen sind in schutzgebenden Konstruktionen verlegt. Der Funktionserhalt der IT-Syste- me und der Datenträger ist bei Umgebungsbränden in Nachbarräumen sichergestellt (EN 1047-2).

Die Risikofaktoren Feuer und Rauchgase lassen sich über Brandmeldeanlagen (DIN EN 54), Brandfrüherkennung (DIN EN 54-20), Brandschutzklappen und Gaslöschtechnik beherrschen. Die Brandmeldesensorik (DIN EN 54) berücksichtigt alle Sicherheitsbereiche und ist an geeigneten Stellen angebracht. Ein Brandschutzkonzept ist mit der örtlichen Feuer- wehr abgestimmt.

Die Brandmeldeanlage (DIN EN 54, VdS 2095, DIN 14675, DIN VDE 833-2) überwacht den gesamten Sicherheitsbe- reich und ist über eine sichere Verbindung bei einer ständig besetzten Stelle aufgeschaltet. Nebenräume, doppelter Fußboden, abgehängte Decken und Luftkanäle sind in die Brandüberwachung einbezogen worden. Wichtig ist, dass ne- ben der Alarmierung Schadensbegrenzungsmaßnahmen ausgelöst werden, etwa durch eine Gaslöschanlage im Sicher- heitsbereich (VdS 2380, VdS 2093) oder durch andere geeignete Maßnahmen.

Die Kommunikationsverkabelung stellt die Verbindung des Rechenzentrums zur Außenwelt dar. Die innere Verkabelung wird je nach Anspruch auf einfachen Wegen bis hin zu redundanter Wegeführung unter Nutzung redundanter, aktiver Komponenten ausgeführt. Kommunikations- und Datenkabel sind gemäß EN 50174-2 mit dem nötigen Abstand zueinan- der auf getrennten Kabelführungen verlegt. Die Verkabelung erfolgt über Haupt-, Bereichs- und Lokalverteiler und erlaubt einen leichten Um- und Ausbau ohne Betriebsunterbrechung. Punkt-zu-Punkt-Verkabelung wird vermieden. Datenkabel werden nicht durch Bereiche mit Gefährdung verlegt oder sind speziell geschützt. WAN-Trassen verlaufen kreuzungsfrei.

Die Energieversorgung ist für die IT-Systeme essentiell. Sie bedient unterschiedlichste Leistungsabnehmer und unterliegt steter Veränderung. Die Elektroinstallation ist auf der Basis der einschlägigen nationalen Normen und Vorschriften (ins- besondere in Deutschland DIN VDE 0100) ausgeführt und gegen Überspannung geschützt. Angepasste Aufteilungen und Absicherungen der Stromkreise sind vorgesehen und Vorkehrungen für Erweiterungen getroffen. Die IT-Systeme werden unterbrechungsfrei mit Strom versorgt (EN 62040 bzw. EN 88528-11). Alle kritischen Infrastrukturen (IT-, Telekommunika- tions-, Sicherheits- und Klimasysteme) sind an eine Notstromversorgung angeschlossen.

MD CLOUD SERVICES GmbH
Sitz der Gesellschaft: Neuss
Handelsregister Neuss HRB-NR. 22400
USt.-ID-Nr. DE 210 900 969

Bank: Commerzbank AG, Neuss
IBAN: DE 11 3004 0000 0752 7500 00
BIC: COBADEFFXXX

Geschäftsführer: Ingo Kalker

Bei der Einspeisung sind Ausweichmöglichkeiten gegeben, wie etwa ein Ringanschluss. Die Elektroinstallation ist im gesamten Gebäude als TN-S-Netz ausgelegt, ansonsten sind besondere Vorkehrungen hinsichtlich der Elektroverteilung zu treffen. Grundsätzlich werden IT-Geräte getrennt von anderen Verbrauchern versorgt. Der Überspannungsschutz ist mindestens in zwei Stufen ausgeführt (VdS 2833), ein Potenzialausgleich (DIN EN 50310) ist sichergestellt und eine Differenzstromüberwachung (DIN EN 62020) in wichtigen Segmenten ist gegeben.

IT-Systeme wie auch Archive und Komponenten der Stromversorgung (USV, Batterien) sind auf bestimmte Umgebungs- bedingungen angewiesen. Lufttemperatur, relative Luftfeuchte und Staubanteil werden innerhalb vorgegebener Gren- zwerte gehalten. Eine Kontamination der Außenluft wird erkannt und ein automatischer Verschluss der Außenluft sicher- gestellt.

Die Grenzwertüberwachung in den IT-Räumen erfolgt redundant. Außenanlagen sind in das Blitzschutzkonzept einge- bunden und sind gegen unbefugten Zutritt geschützt. Eine redundant ausgelegte Klimatisierung erhöht die Verfügbarkeit und ermöglicht Wartungen ohne Betriebsunterbrechung. Die Anlagenteile sind in das Brandschutzkonzept eingebunden. Der Ausfall von Mess-, Steuer- und Regeltechnik ist fehlertolerant ausgelegt. Maßnahmen gegen und zur Detektion von Leckagen sind getroffen. Trassen sind gegen Gefährdungen geschützt. Die Anlagen sind in der Lage, die Wärmeabgabe der IT auch bei hohen Außentemperaturen sicher abzuführen. Der Betrieb der Anlagen wird über eine Gebäudeleittechnik überwacht.

IT-Infrastrukturkomponenten können auch versagen. Die Komponenten werden daher regelmäßigen Überprüfungen des Zustandes und der Eigenschaften unterzogen, um die ständige Wirksamkeit und Verfügbarkeit der Infrastrukturkompo- nenten im Sinne der Sicherheitsanforderungen belegen zu können. Verantwortlichkeiten sind klar definiert.

Verfahrensanweisungen regeln die Prüfung der Auslegung der Elektroinstallation und der raumlufttechnischen Anlagen bei Erweiterungen. Alle Sicherheitseinrichtungen werden regelmäßigen Funktionstests unterzogen. Ein jährlicher War- tungsplan definiert Art und Intervall der Wartung an Verschleißteilen der Infrastrukturkomponenten.

Die Datensicherungsmedien müssen brand- und zugriffsgeschützt getrennt vom Sicherheitsbereich aufbewahrt und ge- mäß EN 1047 ausreichend geschützt werden.

Ein Lifecycle-, sowie ein Kunden-Managementsystem sind eingeführt. Wichtige Schlüsselindikatoren zum sicheren und nachhaltigen, wie auch energieeffizienten Betrieb des Rechenzentrums werden erfasst, ausgewertet und zur Verbesse- rung genutzt.

Die Verfügbarkeit der Daten in unseren Datenverarbeitungssystemen wird durch regelmäßige Datensicherungen ge- währleistet. Die Datensicherungen werden getrennt von produktiven Datenverarbeitungssystemen an einem anderen physikalischen Ort (eigener Brandschutzabschnitt im Rechenzentrum) auf einem separaten Speichersystem gespeichert.

4. VERFAHREN ZUR REGELMÄSSIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG (ART. 32 ABS. 1 LIT. D DSGVO; ART. 25 ABS. 1 DSGVO)

4.1. Datenschutz-Management

Das Unternehmen hat einen externen Datenschutzbeauftragten bestellt und ist per Email unter datenschutz@mdcloudservices.de erreichbar. Es wurde ein Vertrag zur Auftragsverarbeitung (AV-Vertrag) zwischen Verantwortlichen und Auftragsverarbeiter geschlossen.
Das Unternehmen hat alle Mitarbeiter der MD CLOUD SERVICES GmbH zur Wahrung des Datengeheimnisses verpflichtet und führt in regel- mäßigen Abständen Sensibilisierungsmaßnahmen durch.

Das Unternehmen kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach und ein formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden.

Verfahrensanweisungen werden zentral durch ein Managementsystem bereitgestellt.

Externe Dienstleister verpflichten sich der Wahrung des Datengeheimnisses. Die Einhaltung wird seitens der MD CLOUD SERVICES GmbH kontrolliert.

Die TOM werden in regelmäßigen Abständen auf Aktualität und Wirksamkeit geprüft.

4.2. Incident-Response-Management Organisatorische Maßnahmen:

Es existiert ein dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde).
Sicherheitsvorfälle und Datenpannen werden dokumentiert. Technische Maßnahmen: Mehrere Ebenen von Paketfiltern verhindern Einbruchsversuche und ermöglichen im Zusammenspiel mit Einbruchserkennungssystemen die Detektion von Angriffsversuchen.

Emails werden ein- und ausgehend auf Viren geprüft und im Falle von Spam oder erkannten Bedrohungen automatisch ausgefiltert.

MD CLOUD SERVICES GmbH
Sitz der Gesellschaft: Neuss
Handelsregister Neuss HRB-NR. 22400
USt.-ID-Nr. DE 210 900 969

Bank: Commerzbank AG, Neuss
IBAN: DE 11 3004 0000 0752 7500 00
BIC: COBADEFFXXX

Geschäftsführer: Ingo Kalker

4.3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.

4.4. Auftragskontrolle

Das Unternehmen hat einen externen Datenschutzbeauftragten bestellt.

Es wurde ein Vertrag zur Auftragsverarbeitung (AV-Vertrag) zwischen Verantwortlichen und Auftragsverarbeiter abgeschlossen. Das Unternehmen hat alle Mitarbeiter der MD CLOUD SERVICES GmbH zur Wahrung des Datengeheimnisses verpflichtet. Externe Dienstleister verpflichten sich der Wahrung des Datengeheimnisses. Die Einhaltung wird seitens der MD CLOUD SERVICES GmbH kontrolliert.

MD CLOUD SERVICES GmbH
Sitz der Gesellschaft: Neuss
Handelsregister Neuss HRB-NR. 22400
USt.-ID-Nr. DE 210 900 969

Bank: Commerzbank AG, Neuss
IBAN: DE 11 3004 0000 0752 7500 00
BIC: COBADEFFXXX

Geschäftsführer: Ingo Kalker

MD CLOUD SERVICES GmbH

Im Taubental 25
41468 Neuss

Tel: +49 (0) 21 31 - 7 51 98-0
Fax: +49 (0) 21 31 - 7 51 98-99

info@mdcloudservices.de
www.mdcloudservices.de

Anlage 2 zum AV-Vertrag

ZUGELASSENE SUBDIENSTLEISTER

- *pcvisit Software AG, Manfred-von-Ardenne-Ring 20, 01099 Dresden*
- *MK Netzdienste GmbH & Co. KG, Marienwall 27, 32423 Minden*

MD CLOUD SERVICES GmbH
Sitz der Gesellschaft: Neuss
Handelsregister Neuss HRB-NR. 22400
USt.-ID-Nr. DE 210 900 969

Bank: Commerzbank AG, Neuss
IBAN: DE 11 3004 0000 0752 7500 00
BIC: COBADEFFXXX

Geschäftsführer: Ingo Kalker

MD CLOUD SERVICES GmbH

Im Taubental 25
41468 Neuss

Tel: +49 (0) 21 31 - 7 51 98-0
Fax: +49 (0) 21 31 - 7 51 98-99

info@mdcloudservices.de
www.mdcloudservices.de

Anlage 3 zum AV-Vertrag

WEISUNGSBERECHTIGTE PERSONEN

Für die Erteilung von Weisungen ist der Geschäftsführer des Verantwortlichen oder ein von ihm ggf. dem Auftragsverarbeiter schriftlich benannter und bevollmächtigter „technischer Beauftragter“ befugt.

Dies ist namentlich:

1. Herr/Frau _____

2. Herr/Frau _____

3. Herr/Frau _____

4. Herr/Frau _____

5. Herr/Frau _____

Weisungsempfänger beim Auftragsverarbeiter sind die Vorstände, die Geschäftsführer, die Prokuristen, der Datenschutzbeauftragte und Service-Mitarbeiter. Die jeweils aktuellen Kontaktmöglichkeiten sind auf der Website des Auftragsverarbeiters leicht zugänglich hinterlegt.

MD CLOUD SERVICES GmbH
Sitz der Gesellschaft: Neuss
Handelsregister Neuss HRB-NR. 22400
USt.-ID-Nr. DE 210 900 969

Bank: Commerzbank AG, Neuss
IBAN: DE 11 3004 0000 0752 7500 00
BIC: COBADEFFXXX

Geschäftsführer: Ingo Kalker