Besondere Vertragsbestimmungen hinsichtlich der möglichen Auftragsverarbeitung gem. Art. 28 DSGVO zwischen dem Kunden als Verantwortlicher (hier bezeichnet als „Kunde“) und der DQMCLOUD GmbH als Auftragsverarbeiter (hier bezeichnet als „DQMCLOUD“)

Präambel

Der Kunde hat den Auftragnehmer mit den in § 3 genannten Leistungen beauftragt. Teil der Vertragsdurchführung kann die Verarbeitung von personenbezogenen Daten sein. Insbesondere Art. 28 DSGVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien vorsichtshalber die nachfolgende Vereinbarung, deren Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

§ 1 Begriffsbestimmungen

(1) Verantwortlicher ist gem. Art. 4 Abs. 7 DSGVO die Stelle, die allein oder gemeinsam mit anderen Verantwortlichen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

(2) Auftragsverarbeiter ist gem. Art. 4 Abs. 8 DSGVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

(3) Personenbezogene Daten sind gem. Art. 4 Abs. 1 DSGVO 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.

(4) Besonders schutzbedürftige personenbezogene Daten sind personenbezogenen Daten gem. Art. 9 DSGVO, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit von Betroffenen hervorgehen, personenbezogene Daten gem. Art. 10 DSGVO über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln sowie genetische Daten gem. Art. 4 Abs. 13 DSGVO, biometrischen Daten gem. Art. 4 Abs. 14 DSGVO, Gesundheitsdaten gem. Art. 4 Abs. 15 DSGVO sowie Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

(5) Verarbeitung ist gem. Art. 4 Abs. 2 DSGVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte 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.

(6) Aufsichtsbehörde ist gem. Art. 4 Abs. 21 DSGVO eine von einem Mitgliedstaat gem. Art. 51 DSGVO eingerichtete unabhängige staatliche Stelle.

§ 2 Angabe der zuständigen Datenschutz-Aufsichtsbehörde

(1) Die zuständige Aufsichtsbehörde für den Kunden ist im Hauptvertrag dokumentiert.

(2) Zuständige Aufsichtsbehörde für DQMCLOUD ist der Bayerische Landesbeauftragte für den Datenschutz.

(3) Der Kunde und DQMCLOUD arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

§ 3 Vertragsgegenstand

(1) DQMCLOUD erbringt für den Kunden Leistungen im Bereich der Datenqualitätsanalyse auf Grundlage eines elektronisch abgeschlossenen und bei den Parteien jeweils dokumentierten Vertrags

(„Hauptvertrag“). Dabei ist es nicht auszuschließen, dass DQMCLOUD Zugriff auf personenbezogene Daten erhält und diese ausschließlich im Auftrag und nach Weisung des Kunden verarbeitet. Umfang und Zweck der Datenverarbeitung durch DQMCLOUD ergeben sich aus dem Hauptvertrag (und der dazugehörigen Leistungsbeschreibung). Dem Kunden obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung.

(2) Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrags vor.

(3) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei der DQMCLOUD und dessen Beschäftigten oder durch von DQMCLOUD Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Kunden stammen oder für den Kunden erhoben wurden.

(4) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

§ 4 Weisungsrecht

(1) DQMCLOUD darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Kunden erheben, verarbeiten oder nutzen; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird DQMCLOUD durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Kunden diese rechtlichen Anforderungen vor der Verarbeitung mit.

(2) Die Weisungen des Kunden werden anfänglich durch diesen Vertrag festgelegt und können vom Kunden danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Kunde ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten. Die weisungsberechtigten Personen ergeben sich aus dem Hauptvertrag. Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen ist dem Vertragspartner unverzüglich der Nachfolger bzw. Vertreter in Textform zu benennen.

(3) Alle erteilten Weisungen sind sowohl vom Kunden als auch vom Auftragnehmer zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

(4) Ist DQMCLOUD der Ansicht, dass eine Weisung des Kunden gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Kunden unverzüglich darauf hinzuweisen. DQMCLOUD ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Kunden bestätigt oder geändert wird. DQMCLOUD darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

§ 5 Art der verarbeiteten Daten, Kreis der Betroffenen

(1) Im Rahmen der Durchführung des Hauptvertrags erhält DQMCLOUD möglicherweise Zugriff zu personenbezogenen Daten. Diese Daten lassen sich zum Zeitpunkt des Vertragsschlusses noch nicht spezifizieren. Der Kunde ist verpflichtet, im Falle der Inanspruchnahme der Leistungen DQMCLOUD zum Zweck der Verarbeitung von personenbezogenen Daten, eine Spezifikation dieser Daten an DQMCLOUD zu übergeben.

(2) Dasselbe gilt hinsichtlich der Kategorien der von der Datenverarbeitung Betroffenen.

§ 6 Schutzmaßnahmen DQMCLOUD

(1) DQMCLOUD ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Kunden erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

(2) DQMCLOUD wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Kunden gem. Art. 32 DSGVO, insbesondere mindestens die in **Anlage 1** aufgeführten Maßnahmen.

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt DQMCLOUD vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Beim Auftragnehmer ist als betrieblicher Datenschutzbeauftragter/als Ansprechpartner für den Datenschutz (sofern ein Datenschutzbeauftragter nach Art. 37 Abs. 1 DSGVO nicht bestellt werden muss) bestellt:

Information Quality Institute GmbH

Herr Joachim Sobota

Blumenstr. 3

85540 Haar

Germany

datenschutz@dqmcloud.de

(4) Den bei der Datenverarbeitung durch den Auftragnehmer beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. DQMCLOUD wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im folgenden Mitarbeiter genannt), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DSGVO) und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Mitarbeiter und DQMCLOUD bestehen bleiben. Dem Kunden sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

§ 7 Informationspflichten DQMCLOUD

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen von DQMCLOUD, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch DQMCLOUD, bei DQMCLOUD im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird DQMCLOUD den Kunden unverzüglich in Schriftform oder Textform informieren. Dasselbe gilt für Prüfungen von DQMCLOUD durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;

b) eine Beschreibung der von DQMCLOUD ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(2) DQMCLOUD trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informiert hierüber den Kunden und ersucht um weitere Weisungen.

(3) DQMCLOUD ist darüber hinaus verpflichtet, dem Kunden jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Absatz 1 betroffen sind.

(4) Sollten die Daten des Kunden bei DQMCLOUD durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat DQMCLOUD den Kunden unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. DQMCLOUD wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Kunden als Verantwortlichem im Sinne der DSGVO liegen.

(5) Über wesentliche Änderung der Sicherheitsmaßnahmen nach § 6 Abs. 2 hat DQMCLOUD den Kunden unverzüglich zu unterrichten.

(6) Ein Wechsel in der Person des betrieblichen Datenschutzbeauftragten/Ansprechpartners für den Datenschutz ist dem Kunden unverzüglich mitzuteilen.

(7) DQMCLOUD und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag des Kunden durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DSGVO enthält. Das Verzeichnis ist dem Kunden auf Anforderung zur Verfügung zu stellen.

(8) An der Erstellung des Verfahrensverzeichnisses durch den Kunden hat DQMCLOUD im angemessenen Umfang mitzuwirken. Er hat dem Kunden die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

§ 8 Kontrollrechte des Kunden

(1) Der Kunde ist berechtigt, sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen der DQMCLOUD zu überzeugen. Hierfür kann er z. B. Auskünfte von DQMCLOUD einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen von DQMCLOUD nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zu DQMCLOUD steht. Der Kunde wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe bei DQMCLOUD dabei nicht unverhältnismäßig stören.

(2) DQMCLOUD verpflichtet sich, dem Kunden auf dessen mündliche oder schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen von DQMCLOUD erforderlich sind.

(3) Der Kunde dokumentiert das Kontrollergebnis und teilt es DQMCLOUD mit. Bei Fehlern oder Unregelmäßigkeiten, die der Kunde insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Kunde DQMCLOUD die notwendigen Verfahrensänderungen unverzüglich mit.

(4) DQMCLOUD stellt dem Kunden auf dessen Wunsch ein aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung sowie über zugriffsberechtigte Personen zur Verfügung.

(5) DQMCLOUD weist dem Kunden die Verpflichtung der Mitarbeiter nach § 6 Abs. 4 auf Verlangen nach.

§ 9 Einsatz von Subunternehmern

(1) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der in **Anlage 1** genannten Subunternehmer durchgeführt. DQMCLOUD ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt. Er setzt den Kunden hiervon unverzüglich in Kenntnis. DQMCLOUD ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. DQMCLOUD hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass der Kunde seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) direkt gegenüber den Subunternehmern wahrnehmen kann. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat DQMCLOUD sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). DQMCLOUD wird dem Kunden auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

(2) Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn DQMCLOUD Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Server-Housing, Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die DQMCLOUD für den

Kunden erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Subunternehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Kunden genutzt werden und soweit im Rahmen der Wartungs- und Prüfdienstleistungen ein Zugriff auf personenbezogene Daten, die dem Kunden zuzurechnen sind, stattfindet.

§ 10 Anfragen und Rechte Betroffener,

(1) DQMCLOUD unterstützt den Kunden nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12–22 sowie 32 und 36 DSGVO.

(2) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber DQMCLOUD geltend, so reagiert dieser nicht selbstständig, sondern verweist den Betroffenen unverzüglich an den Kunden und wartet dessen Weisungen ab.

§ 11 Haftung

(1) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zu DQMCLOUD alleine der Kunde gegenüber dem Betroffenen verantwortlich.

(2) Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist.

§ 12 Außerordentliches Kündigungsrecht

(1) Der Kunde kann den Hauptvertrag fristlos ganz oder teilweise kündigen, wenn DQMCLOUD seinen Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der DSGVO vorsätzlich oder grob fahrlässig verletzt oder eine Weisung des Kunden nicht ausführen kann oder will. Bei einfachen – also weder vorsätzlichen noch grob fahrlässigen – Verstößen setzt der Kunde DQMCLOUD eine angemessene Frist, innerhalb welcher DQMCLOUD den Verstoß abstellen kann.

§ 13 Beendigung des Hauptvertrags

(1) DQMCLOUD wird dem Kunden nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder – auf Wunsch des Kunden, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Dies betrifft auch etwaige Datensicherungen bei DQMCLOUD. DQMCLOUD hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen. Zu entsorgende Unterlagen sind mit einem Aktenvernichter nach DIN 32757-1 zu vernichten. Zu entsorgende Datenträger sind nach DIN 66399 zu vernichten.

(2) Der Kunde hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren.

(3) DQMCLOUD ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus solange gültig, wie DQMCLOUD über personenbezogene Daten verfügt, die ihm vom Kunden zugeleitet wurden oder die er für diesen erhoben hat.

§ 14 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

(2) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

(3) Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist derjenige des Hauptvertrags.

Anlage1 – Technische und organisatorische Maßnahmen DQMCLOUD / Genehmigte Subunternehmer

1) VERTRAULICHKEIT

Zutrittskontrolle **Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.**	**vorhanden**
Zutrittsberechtigungskonzept	✓
Schlüsselregelung	✓
Begleitung von Besucherzutritten durch eigene Mitarbeiter	✓
Abgestufte Sicherheitsbereiche und kontrollierter Zutritt	✓
Gesondert gesicherter Zutritt zum Rechenzentrum	✓
Aufbewahrung der Server in verschlossenen Räumen	✓
Anweisung zur Ausgabe von Schlüsseln	✓

Zugangskontrolle **Das Eindringen Unbefugter in die DV-Systeme bzw. deren unbefugte Nutzung ist zu verhindern.**	**vorhanden**
Passwortsicherung von Bildschirmarbeitsplätzen	✓
Verwendung von individuellen Passwörtern und SSH-Keys	✓
Automatische Sperrung von Nutzeraccounts nach mehrfacher Fehleingabe von Passwörtern	✓
Automatische passwortgesicherte Sperrung des Bildschirms nach Inaktivität (Bildschirmschoner)	✓
Prozess zur Rechtevergabe bei Neueintritt von Mitarbeitern	✓
Prozess zum Rechteentzug bei Abteilungswechseln von Mitarbeitern	✓
Prozess zum Rechteentzug bei Austritt von Mitarbeitern	✓

Verpflichtung zur Vertraulichkeit	✓
Kontrollierte Vernichtung von Datenträgern	✓
Zugriff auf IT-Systeme ist grundsätzlich nur über passwortgeschützte VPN, IPSec, SSH, SFTP, SSL/TLS Verbindungen (verschlüsselte, authentifizierte Verbindungen) möglich	✓
Jedes IT-System ist durch Firewalls sowie Benutzername und Passwort und/oder Client-Zertifikate vor unberechtigten Zugriffen geschützt. Zugriffe auf die IT-Systeme werden im Access-Log protokolliert und nach Projektanforderung aufbewahrt.	✓

Zugriffskontrolle **Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.**	**vorhanden**
Festlegung der Zugriffsberechtigung, Berechtigungskonzept	✓
Regelung zur Wiederherstellung von Daten aus Backups (wer, wann, auf wessen Anforderung)	✓
Regelmäßige Überprüfung von Berechtigungen	✓
Beschränkung der freien und unkontrollierten Abfragemöglichkeit von Datenbanken	✓
Teilzugriffsmöglichkeiten auf Datenbestände und Funktionen (Read, Write, Execute)	✓
Einsatz von Sicherheitssystemen (Software/Hardware)	✓
▪ Virenscanner	✓
▪ Firewalls	✓
▪ SPAM-Filter	✓
▪ IP Whitelists für kritische Server	✓

Trennungskontrolle **Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.**	vorhanden
Trennung von Kunden (Mandantenfähigkeit des verwendeten Systems)	✓
Logische Datentrennung (z.B. auf Basis von Kunden- oder Mandantennummern)	✓
Berechtigungskonzept, das der getrennten Verarbeitung der Auftraggeber-Daten von	✓

Daten anderer Kunden Rechnung trägt	
Funktionstrennung	✓

2) INTEGRITÄT

Weitergabekontrolle **Aspekte der Weitergabe (Übermittlung) personenbezogener Daten sind zu regeln: Elektronische Übertragung, Datentransport, sowie deren Kontrolle.**	**vorhanden**
Verschlüsselter Datenaustausch	✓
Verschlüsselung vertraulicher Datenträger	✓
Verschlüsselung von Laptopfestplatten	✓
Datenträgerentsorgung - Sichere Löschung von Datenträgern	✓
Papierentsorgung: Sicheres Vernichten von Papierdokumenten	✓
Verpackungs- und Versandvorschriften	✓

Eingabekontrolle **Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten**	**vorhanden**
Festlegung von Benutzerberechtigungen (Profile)	✓
Differenzierte Benutzerberechtigungen (Lesen, Ändern, Löschen)	✓
Teilzugriff auf Daten bzw. Funktionen	✓
Organisatorische Festlegung von Eingabezuständigkeiten	✓
Verpflichtung auf das Datengeheimnis	✓

3) VERFÜGBARKEIT UND BELASTBARKEIT

Verfügbarkeitskontrolle **Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.**	**vorhanden**
Datensicherungs- und Backupkonzepte	✓

Durchführung der Datensicherungs- und Backupkonzepte	✓
Zutrittsbegrenzung in Serverräumlichkeiten auf notwendiges Personal	✓
Brandmeldeanlagen in Serverräumlichkeiten	✓
Rauchmelder in Serverräumlichkeiten	✓
Wasserlose Brandbekämpfungssysteme in Serverräumlichkeiten	✓
Klimatisierte Serverräumlichkeiten	✓
Blitz-/ Überspannungsschutz	✓
CO2 Feuerlöscher in unmittelbarer Nähe der Serverräumlichkeiten	✓
Katastrophen- oder Notfallplan (z.B. Wasser, Feuer, Explosion, Androhung von Anschlägen, Absturz, Erdbeben)	✓
Aufbewahrung der Daten in Datensicherungsschränken, Tresoren	✓
USV-Anlage (Unterbrechungsfreie Stromversorgung)	✓

Widerstandsfähigkeit- und Ausfallsicherheitskontrolle **Systeme müssen die Fähigkeit besitzen mit risikobedingten Veränderungen umgehen zu können und eine Toleranz und Ausgleichsfähigkeit gegenüber Störungen aufweisen.**	**vorhanden**
Redundante Stromversorgung	✓
Redundante USV-Anlage	✓
Festplattenspiegelung	✓
Datenspeicherung auf RAID-Systemen (RAID 1 und höher)	✓
Unverzügliche und regelmäßige Aktivierung von verfügbaren Soft- und Firmwareupdates	✓

4) VERFAHREN ZUR ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

Kontrollverfahren **Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Datensicherheitsmaßnahmen ist zu implementieren**	**vorhanden**

Interne Verfahrensverzeichnisse werden mind. jährlich aktualisiert	✓
Meldung neuer/veränderter Datenverarbeitungsverfahren an den Datenschutzbeauftragten	✓
Es werden datenschutzfreundliche Voreinstellungen gewählt	✓
Getroffene Sicherheitsmaßnahmen werden einer regelmäßigen internen Kontrolle unterzogen	✓
Bei negativem Verlauf der zuvor genannten Überprüfung werden die Sicherheitsmaßnahmen risikobezogen angepasst, erneuert und umgesetzt	✓

Auftragskontrolle **Es ist sicherzustellen, dass Daten die im Auftrag durch Dienstleister (Subauftragnehmer) verarbeitet werden, nur gemäß der Weisung des Auftragnehmers verarbeitet werden.**	**vorhanden**
Vertragsgestaltung gem. gesetzlichen Vorgaben (Art. 28 DSGVO)	✓
Zentrale Erfassung vorhandener Dienstleister (einheitliches Vertragsmanagement)	✓
Regelmäßige Kontrollen beim Auftragnehmer nach Vertragsbeginn (während der Vertragsdauer)	✓

Subunternehmer

Die vertraglich vereinbarten Leistungen oder Teilleistungen werden unter Einschaltung der nachfolgend genannten Subunternehmer durchgeführt:

Firma	**Anschrift**	**Leistungsbeschreibung**
Hetzner Online GmbH	Industriestr. 25 91710 Gunzenhausen Deutschland	Serverprovider Betrieb der Rechenzentren
Mailjet SAS	13-13 bis, Rue de l'Aubrac 75012 Paris Frankreich	Betrieb des Mailservers zum Versenden von Emails über die DQMCloud
Stripe Payment Europe Ltd.	The One Building 1 Grand Canal Street Lower Dublin 2 Irland	Abwicklung der Kreditkartenzahlungen
Fastbill GmbH	Wildunger Str. 6 60487 Frankfurt am Main Deutschland	Abwicklung der Zahlungen via Rechnung
Freshworks, Inc.	1250 Bayhill Drive, Suite 315, San Bruno, CA 94066 USA	Bereitstellung Software as a Service Freshdesk (Bearbeitung von Supportanfragen des Kunden)