Vertrag über die Verarbeitung von Daten im Auftrag

Auftragsverarbeitungsvereinbarung gemäß Art. 28 DSGVO

zwischen

[Name des Auftraggebers / Anschrift des Auftraggebers]

— Auftraggeber —

und

QM Software GmbH

Blocksbergstraße 183

66955 Pirmasens

— Auftragnehmer —

1. Allgemeines

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

(2) Sofern in diesem Vertrag der Begriff „Datenverarbeitung" oder „Verarbeitung" (von Daten) benutzt wird, wird die Definition der „Verarbeitung" im Sinne von Art. 4 Nr. 2 DSGVO zugrunde gelegt.

2. Gegenstand des Auftrags

Art der Verarbeitung

Der Auftragnehmer führt für den Auftraggeber Leistungen aus dem Bereich der Wartung, Pflege, Bereitstellung und des Managements von IT-Systemen, Software und Daten durch. Zwischen den Parteien besteht diesbezüglich ein Vertragsverhältnis („Hauptvertrag"), das auf den Allgemeinen Geschäftsbedingungen der QM Software GmbH sowie den jeweils einschlägigen Besonderen Vertragsbedingungen (BVB) basiert. Diese Vereinbarung beginnt mit Unterzeichnung durch beide Parteien und gilt für die Dauer des jeweiligen Hauptvertrages.

Der Auftrag des Auftraggebers an den Auftragnehmer umfasst insbesondere folgende Arbeiten und/oder Leistungen, soweit im jeweiligen Hauptvertrag vereinbart:

- Cloudbasiertes QM- und Auditsystem als SaaS (QMSpot Cloud / Professional)
- Managed-Service-Leistungen für die QMSpot-Plattform (Managed QM)
- IoT-Konnektivität und Managed-IoT-Leistungen (Bereitstellung von SIM-Karten und Datenübertragung, Geräte-Monitoring, Firmware-Pflege)
- Managed-Workplace-Leistungen für Client-Endgeräte (Patch-Management, Endpoint-Sicherheit, User-Helpdesk)

- Managed-Backup-Leistungen (Datensicherung und Wiederherstellung)
- Managed-Monitoring-Leistungen (technische Überwachung von Servern, Arbeitsplätzen, Netzwerkgeräten)
- Managed-MDM-Leistungen (Verwaltung mobiler Endgeräte)
- Managed-KI-Leistungen (Bereitstellung KI-basierter Funktionen über Azure OpenAI)
- Dienstleistungen wie Onboarding, Schulung, Migration und Beratung

Art der personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1, 13, 14 und 15 DSGVO)

- Name und Kontaktdaten (Beschäftigte, Lieferanten, Kunden des Auftraggebers)
- Aufgaben- und Arbeitspläne, Schulungs- und Qualifikationsdaten, Nachweise
- ggf. durch den Auftraggeber in QMSpot hochgeladene Dokumente mit personenbezogenen Inhalten
- Geräte- und Nutzungsdaten von durch den Auftragnehmer verwalteten Endgeräten (insbesondere im Rahmen von Managed Workplace, Managed MDM, Managed Monitoring)
- Authentifizierungsdaten (Benutzernamen, technische Kennungen) der Anwender
- Inhalte aus Backup-Datenbeständen — diese können sämtliche personenbezogenen Daten umfassen, die der Auftraggeber auf den gesicherten Systemen verarbeitet
- Eingaben in die KI-Plattform (Prompts, hochgeladene Dokumente), soweit der Auftraggeber Managed-KI-Leistungen nutzt
- Sensor- und Geräte-Daten aus IoT-Komponenten

Kreis der von der Datenverarbeitung Betroffenen

- Beschäftigte des Auftraggebers (einschließlich Bewerber, freie Mitarbeiter, Auszubildende, Praktikanten)
- Kunden, Lieferanten und Geschäftspartner des Auftraggebers
- Dritte im Rahmen von hinterlegten Havarie- und Notfallplänen
- weitere Personen, deren Daten der Auftraggeber im Rahmen seiner Geschäftstätigkeit verarbeitet und auf den von uns betreuten Systemen oder in der gesicherten Datenbestand vorhält

Weisungsempfänger beim Auftragnehmer sind:

Timo Müller, Geschäftsführung, +49 261 134 989 10, tm@qmspot.com

3. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Dem Auftragnehmer steht nach Ziff. 4 Abs. 3 das Recht zu, den Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.

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

(3) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen müssen in Textform (z. B. E-Mail) erfolgen.

(4) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.

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

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

4. Allgemeine Pflichten des Auftragnehmers

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

(2) Der Auftragnehmer wird die Datenverarbeitung im Auftrag grundsätzlich in Mitgliedstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchführen. Dem Auftragnehmer ist eine Datenverarbeitung auch außerhalb von EU oder EWR erlaubt, wenn entsprechende Unterauftragnehmer im Drittland unter Einhaltung der Voraussetzungen von Ziff. 9 eingesetzt werden und die Voraussetzungen der Art. 44–48 DSGVO erfüllt sind bzw. eine Ausnahme im Sinne von Art. 49 DSGVO vorliegt.

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

(4) Der Auftragnehmer kann dem Auftraggeber die Person(en) benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind. Sofern weisungsempfangsberechtigte Personen benannt werden sollen, werden diese in der Anlage 1 benannt. Für den Fall, dass sich die weisungsempfangsberechtigten Personen beim Auftragnehmer ändern, wird der Auftragnehmer dies dem Auftraggeber in Textform mitteilen.

5. Datenschutzbeauftragter des Auftragnehmers

(1) Der Auftragnehmer bestätigt, dass er einen Datenschutzbeauftragten nach Art. 37 DSGVO benannt hat. Der Auftragnehmer trägt Sorge dafür, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt.

(2) Die Pflicht zur Benennung eines Datenschutzbeauftragten nach Absatz 1 kann im Ermessen des Auftraggebers entfallen, wenn der Auftragnehmer nachweisen kann, dass er gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu bestellen und der Auftragnehmer nachweisen kann, dass betriebliche Regelungen bestehen, die eine Verarbeitung personenbezogener Daten unter Einhaltung der gesetzlichen Vorschriften, der Regelungen dieses Vertrages sowie etwaiger weiterer Weisungen des Auftraggebers gewährleisten.

6. Meldepflichten des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen. Gleiches gilt für jede Verletzung des Schutzes personenbezogener Daten, die der Auftragnehmer im Auftrag des Auftraggebers verarbeitet.

(2) Ferner wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betreffen kann.

(3) Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei der Umsetzung der Meldepflichten unterstützen. Der Auftragnehmer wird dem Auftraggeber insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, unverzüglich ab Kenntnis des Zugriffs mitteilen. Die Meldung des Auftragnehmers an den Auftraggeber muss insbesondere folgende Informationen beinhalten:

- 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 Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

7. Mitwirkungspflichten des Auftragnehmers

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

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

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

8. Kontrollbefugnisse

(1) Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer im erforderlichen Umfang zu kontrollieren.

(2) Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle im Sinne des Absatzes 1 erforderlich ist.

(3) Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragnehmers durch die Kontrollen nicht unverhältnismäßig zu stören. Die Parteien gehen davon aus, dass eine Kontrolle höchstens einmal jährlich erforderlich ist. Weitere Prüfungen sind vom Auftraggeber unter Angabe des Anlasses zu begründen. Im Falle von Vor-Ort-Kontrollen wird der Auftraggeber dem Auftragnehmer die entstehenden Aufwände inkl. der Personalkosten für die Betreuung und Begleitung der Kontrollpersonen vor Ort in angemessenem Umfang ersetzen. Die Grundlagen der Kostenberechnung werden dem Auftraggeber vom Auftragnehmer vor Durchführung der Kontrolle mitgeteilt.

(4) Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen anstatt einer Vor-Ort-Kontrolle auch durch die Vorlage eines geeigneten, aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung (z. B. ISO/IEC 27001) erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der technischen und organisatorischen Maßnahmen gemäß Anlage 2 zu diesem Vertrag zu überzeugen. Sollte der Auftraggeber begründete Zweifel an der Eignung des Prüfdokuments im Sinne des Satzes 1 haben, kann eine Vor-Ort-Kontrolle durch den Auftraggeber erfolgen. Dem Auftraggeber ist bekannt, dass eine Vor-Ort-Kontrolle in Rechenzentren nicht oder nur in begründeten Ausnahmefällen möglich ist.

(5) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber im Sinne von Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Auftraggeber ist über entsprechende geplante Maßnahmen vom Auftragnehmer zu informieren.

9. Unterauftragsverhältnisse

(1) Der Auftragnehmer ist berechtigt, die in der Anlage 1 zu diesem Vertrag angegebenen Unterauftragnehmer für die Verarbeitung von Daten im Auftrag einzusetzen. Der Wechsel von Unterauftragnehmern oder die Beauftragung weiterer Unterauftragnehmer ist unter den in Absatz 2 genannten Voraussetzungen zulässig.

(2) Der Auftragnehmer hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Der Auftragnehmer wird den Auftraggeber im Falle eines geplanten Wechsels eines Unterauftragnehmers oder bei geplanter Beauftragung eines neuen Unterauftragnehmers rechtzeitig, spätestens aber 4 Wochen vor dem Wechsel bzw. der Neubeauftragung in Textform informieren („Information"). Der Auftraggeber hat das Recht, dem Wechsel oder der Neubeauftragung des Unterauftragnehmers unter Angabe einer Begründung in Textform binnen drei Wochen nach Zugang der „Information" zu widersprechen. Der Widerspruch kann vom Auftraggeber jederzeit in Textform zurückgenommen werden. Im Falle eines Widerspruchs kann der Auftragnehmer das Vertragsverhältnis mit dem Auftraggeber mit einer Frist von mindestens 14 Tagen zum Ende eines Kalendermonats kündigen. Der Auftragnehmer wird bei der Kündigungsfrist die Interessen des Auftraggebers angemessen berücksichtigen. Wenn kein Widerspruch des Auftraggebers binnen drei Wochen nach Zugang der „Information" erfolgt, gilt dies als Zustimmung des Auftraggebers zum Wechsel bzw. zur Neubeauftragung des betreffenden Unterauftragnehmers.

(3) Der Auftragnehmer ist verpflichtet, sich vom Unterauftragnehmer bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten gemäß Art. 37 DSGVO benannt hat, sofern der Unterauftragnehmer zur Benennung eines Datenschutzbeauftragten gesetzlich verpflichtet ist.

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

(5) Der Auftragnehmer hat mit dem Unterauftragnehmer einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Darüber hinaus hat der Auftragnehmer dem Unterauftragnehmer dieselben Pflichten zum Schutz personenbezogener Daten aufzuerlegen, die zwischen Auftraggeber und Auftragnehmer festgelegt sind. Dem Auftraggeber ist der Auftragsdatenverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.

(6) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 8 dieses Vertrages) des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Auftraggeber und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

(7) Nicht als Unterauftragsverhältnisse im Sinne der Absätze 1 bis 6 sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne

konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. Der Auftragnehmer ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten. Die Wartung und Pflege von IT-Systemen oder Applikationen stellt ein zustimmungspflichtiges Unterauftragsverhältnis und Auftragsverarbeitung im Sinne von Art. 28 DSGVO dar, wenn die Wartung und Prüfung solche IT-Systeme betrifft, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden und bei der Wartung auf personenbezogene Daten zugegriffen werden kann, die im Auftrag des Auftraggebers verarbeitet werden.

10. Vertraulichkeitsverpflichtung

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet.

(2) Der Auftragnehmer hat seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut gemacht und zur Vertraulichkeit verpflichtet.

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

11. Wahrung von Betroffenenrechten

(1) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei seiner Pflicht, Anträge von Betroffenen nach Art. 12–23 DSGVO zu bearbeiten, zu unterstützen. Der Auftragnehmer hat dabei insbesondere Sorge dafür zu tragen, dass die insoweit erforderlichen Informationen unverzüglich an den Auftraggeber erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DSGVO nachkommen kann.

(2) Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten — insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung — durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen. Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

(3) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Auftraggeber beim Auftragnehmer entstehen, bleiben unberührt.

12. Geheimhaltungspflichten

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

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

13. Vergütung

Die Vergütung des Auftragnehmers wird gesondert vereinbart.

14. Technische und organisatorische Maßnahmen zur Datensicherheit

(1) Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO. Der Auftragnehmer ist im Geschäftsbereich QMSpot (Softwareentwicklung und Cloud-Betrieb) nach ISO/IEC 27001 zertifiziert (Stand: März 2026); die Zertifizierung umfasst den gesamten Produkt-Lifecycle von der Entwicklung bis zum Hosting des QMSpot-Produkts. Im Geschäftsbereich ITSpot werden die technischen und organisatorischen Maßnahmen entsprechend den Vorgaben des ISO/IEC 27001-Standards umgesetzt; ITSpot setzt für die operative Erbringung der Leistungen ausschließlich nach ISO/IEC 27001 zertifizierte Partner ein (insbesondere Microsoft Ireland Operations Limited und Hetzner Online GmbH).

(2) Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als Anlage 2 zu diesem Vertrag beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Voraus mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann einmal jährlich oder bei begründeten Anlässen eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

15. Dauer des Auftrags

(1) Der Vertrag beginnt mit Unterzeichnung und läuft für die Dauer des zwischen den Parteien bestehenden Hauptvertrages über die Nutzung der Dienstleistungen des Auftragnehmers durch den Auftraggeber.

(2) Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

16. Beendigung

(1) Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem

Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren.

(2) Der Auftragnehmer darf personenbezogene Daten, die im Zusammenhang mit dem Auftrag verarbeitet worden sind, über die Beendigung des Vertrages hinaus speichern, wenn und soweit den Auftragnehmer eine gesetzliche Pflicht zur Aufbewahrung trifft. In diesen Fällen dürfen die Daten nur für Zwecke der Umsetzung der jeweiligen gesetzlichen Aufbewahrungspflichten verarbeitet werden. Nach Ablauf der Aufbewahrungspflicht sind die Daten unverzüglich zu löschen.

17. Zurückbehaltungsrecht

Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer im Sinne von § 273 BGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird.

18. Schlussbestimmungen

(1) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

(2) Für Nebenabreden ist die Textform erforderlich.

(3) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

_____ _____

Datum, Unterschrift Auftraggeber Datum, Unterschrift Auftragnehmer

QM Software GmbH
Blocksbergstraße 183
66955 Pirmasens

Fon: +49 261 134 989 10
E-Mail: info@qmspot.com
Web: qmspot.com

Bank 1 Saar eG
IBAN: DE92 5919 0000 0126 4670 01
BIC: SABADE5SXXX

Amtsgericht München
Registernummer: HRB: 284652
USt-IdNr.: DE361579292

Geschäftsführer
Timo Müller
Peter Scharf

Anlage 1 zu AVV QMSoftware: Unterauftragnehmer

Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer").

Dabei handelt es sich um die nachfolgenden Unternehmen:

Hosting QMSpot-Cloud und Azure OpenAI Service (Managed KI)

Microsoft Ireland Operations Limited

70 Sir John Rogerson's Quay

Dublin 2, Irland

Eingetragen in Irland mit der Nummer 256796

Tätigkeit: Hosting der QMSpot-Cloud-Infrastruktur sowie Bereitstellung des Azure OpenAI Service für Managed-KI-Leistungen. Die Verarbeitung erfolgt in einer Azure-Region innerhalb der Europäischen Union; die konkrete Region wird vor Vertragsbeginn vereinbart und dokumentiert. Zertifizierung: ISO/IEC 27001. Drittlandsbezug: keiner.

Hosting Managed-Backup-Infrastruktur

Hetzner Online GmbH

Industriestraße 25

91710 Gunzenhausen

Deutschland

Tätigkeit: Bereitstellung der Server- und Storage-Infrastruktur für Managed-Backup-Leistungen. Standort des Rechenzentrums: Nürnberg, Deutschland. Zertifizierung: ISO/IEC 27001. Drittlandsbezug: keiner.

CRM-System

HubSpot, Inc.

25 First Street

Cambridge, MA 02141

USA

Tätigkeit: Bereitstellung des CRM-Systems für die Geschäftskommunikation. Drittlandsbezug: ja (USA); Datenübermittlung erfolgt unter Einhaltung der Voraussetzungen des EU-US Data Privacy Framework.

QM Software GmbH
Blocksbergstraße 183
66955 Pirmasens

Fon: +49 261 134 989 10
E-Mail: info@qmspot.com
Web: qmspot.com

Bank 1 Saar eG
IBAN: DE92 5919 0000 0126 4670 01
BIC: SABADE5SXXX

Amtsgericht München
Registernummer: HRB: 284652
USt-IdNr.: DE361579292

Geschäftsführer
Timo Müller
Peter Scharf

Anlage 2 zu AVV QMSoftware: Technische und organisatorische Maßnahmen

Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung nachfolgender technischer und organisatorischer Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Der Auftragnehmer ist im Geschäftsbereich QMSpot nach ISO/IEC 27001 zertifiziert (Stand: März 2026). Die nachfolgenden Maßnahmen werden geschäftsbereichsübergreifend umgesetzt und gelten gleichermaßen für den Geschäftsbereich ITSpot; ITSpot setzt für die operative Erbringung der Leistungen überwiegend und nach Möglichkeit nach ISO/IEC 27001 zertifizierte Partner ein.

a) Zutrittskontrolle

Maßnahmen, mit denen Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt wird:

- Zentrale Systeme stehen entweder im eigenen Serverraum oder werden in Rechenzentren von Microsoft (QMSpot-Cloud, Azure OpenAI) bzw. Hetzner (Managed-Backup) verarbeitet.
- Der eigene Serverraum ist durch eine Schließanlage abgesichert und nur berechtigte Personen haben Zutritt.
- Der Serverraum ist nur durch das interne Treppenhaus erreichbar. Der Zugang erfolgt über drei aufeinander folgende Türen abgesichert (1. Tür: Schließanlage Haupteingang; 2. Tür: physischer Schlüssel (Herausgabe nur für Berechtigte durch Tresor); 3. Tür: physischer Schlüssel (Herausgabe nur für Berechtigte durch Tresor).
- Die Büroräume sind durch eine Schließanlage gesichert. Schlüssel bzw. biometrische Zugänge werden durch die IT-Leitung berechtigt und ausgegeben.
- Datensicherungen werden in einem anderen Brandabschnitt als der Serverraum gelagert.

b) Zugangskontrolle

Maßnahmen, mit denen die Nutzung von Datenverarbeitungssystemen durch Unbefugte verhindert wird:

- Für alle IT-Systeme im Unternehmen werden eindeutige Benutzernamen und individuelle Passwörter vergeben.
- Mehr-Faktor-Authentifizierung (MFA) wird für administrative Zugriffe und für Zugriffe auf Cloud-Dienste (Microsoft 365, Azure, Hetzner) eingesetzt.
- Das Unternehmensnetzwerk ist durch eine Firewall mit integriertem IDS / IPS geschützt.
- Sowohl Server als auch Clients sind mit einem angemessenen Virenschutz ausgestattet.
- Der Zugang von einem Heimarbeitsplatz auf IT-Systeme des Unternehmens geschieht mittels einer gesicherten VPN-Verbindung.
- Es existiert eine Gruppenrichtlinie für alle Client-PCs, die nach drei Minuten Inaktivität automatisch den Bildschirm sperrt.
- Systeme werden nach dreimaliger Falscheingabe des Passwortes automatisch gesperrt.
- Ein Passwortmanager wird unternehmensweit eingesetzt.

c) Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugangsberechtigung 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:

- Im Rahmen des formularbasierten Check-In-Prozesses werden vom Vorgesetzten die einzelnen Systemberechtigungen für neue Mitarbeiter genehmigt und zentral von der Betriebs-/ bzw. IT-Leitung vergeben.
- Durch den formularbasierten Check-Out-Prozess wird sichergestellt, dass beim Ausscheiden eines Mitarbeiters alle Berechtigungen entzogen und alle IT-Systeme sowie Datenträger zurückgegeben werden.
- Mit Hilfe eines zertifizierten Dokumentenvernichtungs-Unternehmens (Sicherheitsstufe P-4) wird sichergestellt, dass sensible und personenbezogene Dokumente, die nicht mehr benötigt werden, sicher entsorgt werden.

d) Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

- Die Weitergabe personenbezogener Daten erfolgt ausschließlich verschlüsselt (TLS für Datenübertragung, Verschlüsselung at-rest in den Rechenzentren).
- Im Rahmen von Fehleranalysen und Supporttätigkeiten erfolgt der Zugriff auf Kundensysteme grundsätzlich nach dem Prinzip der Datensparsamkeit und nur mit dokumentiertem Anlass.
- Externe Datenträger (USB-Sticks, externe Festplatten) für den Transport personenbezogener Daten werden nicht eingesetzt.
- Übermittlungen an Subunternehmer (vgl. Anlage 1) erfolgen ausschließlich verschlüsselt.

e) Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt werden:

- Alle zentralen Server-Systeme erstellen Log-Files, die zentral gesammelt und auswertbar abgelegt werden (SIEM-fähige Loginfrastruktur).
- Anlassbezogene und stichprobenartige Auswertungen der Log-Files erfolgen durch die IT-Sicherheit bzw. den Datenschutzbeauftragten.

f) Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:

- Es existieren mit allen Subunternehmern AV-Verträge nach Art. 28 DSGVO.

g) Verfügbarkeitskontrolle

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

- Alle Server stehen in speziellen Räumen bzw. Rechenzentren, die mittels unterbrechungsfreier Stromversorgung (USV) mit Überspannungsschutz, Rauchmelder, Klimatisierung und automatischen Sensoren zur Temperaturüberwachung ausgestattet sind.
- Es werden regelmäßig Datensicherungen vorgenommen und auf Rückspielbarkeit verifiziert. Die Medien der Datensicherung werden in einem anderen Brandabschnitt sicher aufbewahrt.
- Für wichtige Systeme existieren Wartungsverträge, welche die externe Unterstützung bei Problemen regeln.

h) Trennungsprinzip

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

Die Daten unterschiedlicher Auftraggeber werden in logisch voneinander getrennten Systemen gespeichert und verarbeitet. Gleiches gilt für Daten eines Auftraggebers, die zu unterschiedlichen Zwecken erhoben und verarbeitet werden. Konkret wird die Trennung durch unterschiedliche Datenbanken, Server und Storage-Accounts realisiert.

i) Datenschutzmanagement

Der Auftragnehmer hat einen externen Datenschutzbeauftragten bestellt. Dieser ist für das Datenschutzmanagement zuständig und informiert den Auftragnehmer regelmäßig über aktuelle rechtliche Entwicklungen und die daraus abzuleitenden Maßnahmen. Sämtliche mit der Verarbeitung personenbezogener Daten betraute Mitarbeiter des Auftragnehmers werden zum Datenschutz verpflichtet und in der Einhaltung der Regelungen unterwiesen. Außerdem sind alle Mitarbeiter des Auftragnehmers zur Vertraulichkeit verpflichtet. Der Auftragnehmer ist im Geschäftsbereich QMSpot nach ISO/IEC 27001 zertifiziert; die Zertifizierung wird in regelmäßigen Audits aufrechterhalten.

j) Datenschutzfreundliche Voreinstellungen

Die Verarbeitung personenbezogener Daten erfolgt stets nach dem Minimalitätsprinzip. Es werden nur Daten erhoben und verarbeitet, die für die jeweiligen Prozesse erforderlich sind.

QM Software GmbH
Blocksbergstraße 183
66955 Pirmasens

Fon: +49 261 134 989 10
E-Mail: info@qmspot.com
Web: qmspot.com

Bank 1 Saar eG
IBAN: DE92 5919 0000 0126 4670 01
BIC: SABADE5SXXX

Amtsgericht München
Registernummer: HRB: 284652
USt-IdNr.: DE361579292

Geschäftsführer
Timo Müller
Peter Scharf