Vereinbarung zur Auftragsverarbeitung

Hiermit beauftrage ich als Auftraggeber und unter Bezugnahme auf den parallel geschlossenen Internet-Dienstleistungsvertrag die

ieQ-systems SHK GmbH & Co. KG,
Fridtjof-Nansen-Weg 8,
48155 Münster

- nachstehend Auftragnehmer genannt –

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

- Betreuung, Wartung und Hosting unseres Internet-Auftritts inklusive diverser Kontaktmöglichkeiten, exemplarisch
    - Kontaktformulare
    - Terminkalender
    - Online-Bewerbung
    - Merkliste
- Betreuung Stammkunden-Info

(2) Die Dauer dieses Auftrags wird auf unbestimmte Zeit erteilt.

Gleichwohl kann der Auftraggeber die Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

(3) Der Auftragnehmer erklärt, dass er in der Lage ist, die aufgetragenen Daten nach Maßgabe der Artt. 28 bis 36 DS-GVO ordnungsgemäß und gewissenhaft durchzuführen.

2. Konkretisierung der Auftragsverarbeitung

(1) Der Umfang der durchzuführenden Arbeiten erstreckt sich auf die unter 1. (1) angegebenen Tätigkeiten zum Zweck

- ordnungsgemäßen Außendarstellung des Auftraggebers im World-Wide-Web und dem rechtskonformen Umgang mit dem Marketinginstrument Stammkunden-Info.

(2) Art der Verarbeitung personenbezogener Daten sind Personenstamm- und Kommunikationsdaten (z. B. Telefon, E-Mail).

(3) Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen Kunden und Interessenten sowie Bewerber.

(4) Die Erbringung der Datenverarbeitung im Auftrag findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einer oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DS-GVO erfüllt sind.

Das angemessene Schutzniveau in Deutschland ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DS-GVO).

3. Technisch-organisatorische Maßnahmen

(1) Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogene Daten oder Datenkategorien geeignet sind.

(2) Daher werden die in der Anlage beschriebenen technisch-organisatorischen Maßnahmen des Auftragnehmers als verbindlich festgelegt.

(3) Der Auftragnehmer beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.

(4) Die Datensicherheitsmaßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden.

(5) Wesentliche Änderungen sind vom Auftragnehmer mit dem Auftraggeber schriftlich abzustimmen.

4. Berichtigung, Sperrung und Löschung von Daten

Bei der Verarbeitung personenbezogener Daten achtet der Auftragnehmer insbesondere darauf, dass im Sinne der DS-GVO eine ggf. nötige Berichtigung, Sperrung und Löschung personenbezogener Daten durchgeführt wird. Im Zweifelsfall wird der Auftraggeber den Auftragnehmer informieren.

5. Pflichten des Auftragnehmers und deren Kontrollen

(1) Die Pflichten des Auftragnehmers ergeben sich aus Artt. 28 bis 33 DS-GVO, insbesondere die durch den Auftragnehmer durchzuführenden Kontrollen. Die bei der Datenverarbeitung eingesetzten Mitarbeiter des Auftragnehmers müssen schriftlich auf die Grundsätze des Art. 5 Abs. 1 DS-GVO verpflichtet werden.

(2) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers. Der Auftragnehmer verwendet die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt.

(3) Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

(4) Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden Verwaltung. Eingang und Ausgang werden dokumentiert.

(5) Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind mit dem Auftraggeber abzustimmen.

(6) Soweit die beim Auftragnehmer getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.

(7) Der Auftragnehmer hat über die gesamte Abwicklung der Dienstleistung für den Auftraggeber insbesondere folgende Kontrollen in seinem Bereich durchzuführen: Einhaltung der in der Anlage beschriebenen technischen und organisatorischen Maßnahmen.

(8) An der Erstellung der Verarbeitungsverzeichnisse des Auftraggebers (Art. 30 DS-GVO) hat der Auftragnehmer mitzuwirken.

(9) Er hat die erforderlichen Angaben dem Auftraggeber zuzuleiten.

(10) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt.

(11) Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

(12) Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Sicherheitskontrollen vor Ort.

(13) Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Artt. 12 bis 22 DS-GVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

(14) Beim Auftragnehmer ist als Beauftragter für den Datenschutz Herr Rechtsanwalt Carsten Stemberg, Rechtsabteilung, 0251 606 560 12 18, bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z. B. als Telekommunikationsleistungen, Post-/ Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

(5) Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

Firma Unterauftragnehmer	Anschrift / Land	Leistung
GLOBE Development GmbH	Königsberger Straße 260, 48157 Münster Deutschland	Hosting der Webseite

7. Kontrollrechte des Auftraggebers, Duldungs- und Mitwirkungspflichten

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, können durch jährliche Testate des Auftragnehmers erfolgen.

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

8. Mitteilung bei Verstößen des Auftragnehmers

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Artt. 33 und 34 DS-GVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Artt. 33 und 34 DS-GVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DS-GVO). Meldungen nach Artt. 33 oder 34 DS-GVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gemäß nachfolgender Regelung dieser Vereinbarung durchführen.

9. Weisungsbefugnis des Auftraggebers

Der Auftragnehmer verpflichtet sich, die Verarbeitung der ihm übergebenen personenbezogenen Daten ausschließlich im Rahmen der vertraglich festgelegten Weisungen des Auftraggebers durchzuführen. Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen das Bundesdatenschutzgesetz oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit seine Daten und Unterlagen betroffen sind.

10. Löschung und Rückgabe von personenbezogenen Daten

Nicht mehr erforderliche Daten sind beim Auftragnehmer unverzüglich zu löschen. Bei Beendigung des Auftragsverhältnisses verpflichtet sich der Auftragnehmer, alle ihm in Zusammenhang mit dem Auftrag übergebenen und bis dahin noch nicht verarbeiteten bzw. gelöschten personenbezogenen Daten an den Auftraggeber zurückzugeben bzw. den Nachweis einer ordnungsgemäßen Vernichtung darüber zu führen. Es wird gewährleistet, dass zur Verarbeitung / Löschung bestimmte Datenträger während ihres Transportes gegen unberechtigte Einsichtnahme und Verlust geschützt sind. Eine notwendige endgültige Löschung der verbliebenen personenbezogenen Daten wird vom Auftragnehmer unmittelbar nach Beendigung des Auftrags durchgeführt.

11. Sonstiges

(1) Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

(2) Die Einrede des Zurückbehaltungsrechts wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(3) Es gilt das Recht der Bundesrepublik Deutschland.

(4) Als Gerichtsstand wird Münster / Westfalen vereinbart.

12. Schlussbestimmungen

(1) Abweichende oder ergänzende Bestimmungen sowie Nebenabreden oder Änderungen gelten nur, wenn sie schriftlich vereinbart werden.

(2) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder zum Teil unwirksam sein oder werden, wird davon die Wirksamkeit der übrigen Bestimmungen nicht berührt. Die Vertragspartner sind in diesem Fall verpflichtet, die Bestimmungen so auszulegen und zu gestalten, dass der mit den nichtigen oder rechtsunwirksamen Teilen angestrebte Erfolg soweit als möglich erreicht wird.

Anlage – Technisch-organisatorische Maßnahmen

Stand: Juni 2020

1. Zutrittskontrolle

Ziel der Zutrittskontrolle ist es, dass Unbefugten der Zutritt zu solchen Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet oder genutzt werden. Es existieren folgende Maßnahmen zur Zutrittskontrolle:

- Alarmanlage
- manuelles Schließsystem
- Sicherheitsschlösser
- Schlüsselregelung (Schlüsselausgabe etc.)
- Bewegungsmelder
- Wachdienst
- sorgfältige Auswahl von Wach- und Reinigungspersonal

2. Zugangskontrolle

Ziel der Zugangskontrolle ist es zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden, mit denen die Verarbeitung und Nutzung personenbezogener Daten durchgeführt werden. Es existieren folgende Maßnahmen zur Zugangskontrolle:

- Erstellen von Benutzerprofilen
- Zuordnung von Benutzerrechten
- Benutzerberechtigungen verwalten (z.B. bei Eintritt, Austritt, Änderung)
- Passwortvergabe
- Authentifikation mit Benutzername / Passwort
- Einsatz von VPN-Technologie
- Sperren von externen Schnittstellen (USB etc.)
- Schlüsselregelung (Schlüsselausgabe etc.)
- Verschlüsselung von mobilen Datenträgern
- Verschlüsselung von Smartphone-Inhalten
- Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)
- Verschlüsselung von Datenträgern in Laptops / Notebooks
- Einsatz von Anti-Viren-Software
- Einsatz einer Hardware-Firewall
- Einsatz einer Software-Firewall bei allen mobilen Arbeitsplätzen

3. Zugriffskontrolle

Die Maßnahmen zur Zugriffskontrolle müssen darauf ausgerichtet sein, dass nur auf Daten zugegriffen werden kann, für die eine Zugriffsberechtigung besteht und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Es existieren folgende Maßnahmen zur Zugriffskontrolle:

- Erstellen eines Berechtigungskonzepts
- Verwaltung der Rechte durch Systemadministrator
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- physische Löschung von Datenträgern vor Wiederverwendung
- ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)
- Einsatz von Aktenvernichtern
- Protokollierung der Vernichtung von Festplatten

- Verschlüsselung von Datenträgern

4. Weitergabekontrolle

Ziel der Weitergabekontrolle ist es zu 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. Es existieren folgende Maßnahmen zur Weitergabekontrolle:

- Einrichtungen von Standleitungen bzw. VPN-Tunneln
- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
- sichere Transportbehälter/-verpackungen bei physischem Transport

5. Eingabekontrolle

Ziel der Eingabekontrolle ist es, mit Hilfe geeigneter Maßnahmen sicherzustellen, dass nachträglich die näheren Umstände der Dateneingabe überprüft und festgestellt werden können. Es existieren folgende Maßnahmen zur Eingabekontrolle:

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

6. Verfügbarkeitskontrolle

Ziel der Verfügbarkeitskontrolle ist es, zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Es existieren folgende Maßnahmen zur Verfügbarkeitskontrolle:

- Unterbrechungsfreie Stromversorgung (USV)
- Klimaanlage in Serverräumen
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte in Serverräumen
- Erstellen eines Backup- & Recoverykonzepts
- Testen von Datenwiederherstellung
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Serverräume nicht unter sanitären Anlagen

7. Trennungskontrolle

Die Maßnahmen zur Trennungskontrolle müssen darauf ausgerichtet sein zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Es existieren folgende Maßnahmen zur Trennungskontrolle:

- physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- logische Mandantentrennung (softwareseitig)
- Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- Festlegung von Datenbankrechten

- Trennung von Produktiv- und Testsystem

8. Auftragskontrolle

Ziel der Auftragskontrolle ist es zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Kunden verarbeitet werden können. Es existieren folgende Maßnahmen zur Auftragskontrolle:

- Auftragsdatenverarbeitungsvertrag
- Auftragnehmer hat Datenschutzbeauftragten bestellt
- wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
- Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten