Auftragsverarbeitung gemäß Art. 28 DS-GVO

Vereinbarung

Zwischen

Awenko GmbH & Co. KG
Gesellschaft für anwendbare Konzepte
Brägeler Str. 98
49393 Lohne

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

und

Muster Gesundheitsamt

- Verantwortlicher - nachstehend Auftraggeber genannt -

1. Gegenstand und Dauer des Auftrags

I. Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: Bereitstellungen einer web- und appbasierten Software zur Dokumentation des Qualitätsmanagements sowie zur Planung und Durchführung vielseitiger dokumentierbarer Audits und Kontrollen. Zusätzlich kann es zu Fernwartungsdienstleistungen im Bereich der Fehlerbehebung kommen. Der genaue Umfang des Softwarepaketes ist der Auftragsbestätigung zu entnehmen.

II. Der Auftrag wird für die Zeitspanne des Hauptvertrages abgeschlossen. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

2. Konkretisierung des Auftragsinhalts

I. Art und Zweck der vorgesehenen Verarbeitung von Daten:
Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers:
Der Auftragnehmer stellt dem Auftraggeber eine web- und appbasierte Lösung zur Dokumentation von Qualitätsmanagementaudits sowie individualisierbarer elektronischer Dokumentationsmöglichkeiten bereit.

Hierbei können in der App mehrere verschiedene Funktionen genutzt werden:

- Ticketsystem
- Qualitätsaufzeichnungen
- Alarmierung bei Soll-Ist-Abweichungen oder Störungen
- Dokumenten- und Datenarchiv

- Formblätter und Checklisten
- Lieferantenbewertungen
- Daten zu Wartungen und Instandhaltungen
- Kundenumfragen
- Prüfmittelüberwachung
- Individuell erstellte Prüf- und Aufzeichnungsprozesse

Die webbasierte Lösung beinhaltet:

- Übersicht / Dashboard
- Zugangsverwaltung
- Erstellung von Prüf- und Auditberichten
- Berichtswesen
- Schnittstellen

Der genaue Softwareumfang ist der Auftragsbestätigung des zugehörigen Auftrages zu entnehmen.
Die Wartung und Pflege der Serversysteme übernimmt der Auftragnehmer in Abstimmung mit dem Auftraggeber.
Fernwartungsarbeiten zur Fehlerbehebung können nach Maßgabe des Auftraggebers durchgeführt werden.
Je nach Rechtevergabe durch den Auftraggeber kann die unter Punkt 3 genannte betroffenen Gruppe variieren.
Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.
Das angemessene Schutzniveau in Deutschland ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DS-GVO).

II. Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien):

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail, Adressbücher)
- Planungs- und Steuerungsdaten
- Fotos
- Unternehmensdaten (Dokumentation der am Projekt beteiligten)
- Protokollierte Tätigkeiten
- Abweichungsberichte jeglicher Art

III. Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Kunden
- Beschäftigte
- Lieferanten
- Ansprechpartner
- Dienstleister

3. Technisch-organisatorische Maßnahmen

I. Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung,

insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

II. Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].

III. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

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

II. Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

I. Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

II. Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 28 und 29 DS-GVO ausübt. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

Datenschutzbeauftragter der Awenko GmbH & Co. KG:
Secom IT GmbH GmbH, Marc Friedrich, Nienburger Straße 9d, 27232 Sulingen
Kontakt per Mail: datenschutz@secom-it.de, per Tel: 04271- 94738 00

III. Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum

Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

IV. Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].

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

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

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

VIII. Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

I. 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-/Transport-dienstleistungen, 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.

II. Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) grundsätzlich nur dann beauftragen, wenn er selbst sichergestellt hat, dass der Unterauftragnehmer die nötigen gesetzlichen Anforderungen erfüllt. Die eingesetzten Unterauftragnehmer sind in der Anlage 2 aufzuführen.

III. Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine

Unterbeauftragung gestattet.

IV. Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

V. 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.

7. Kontrollrechte des Auftraggebers

I. 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.

II. 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.

III. Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch
- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

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

8. Mitteilung bei Verstößen des Auftragnehmers

I. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.:
   a. die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
   b. die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
   c. die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
   d. die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
   e. die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

II. Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder auf ein Fehlverhalten des Auftraggebers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

I. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

II. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

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

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

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

Datum	Auftraggeber
Datum	Auftragnehmer

Anlage 1 – Technisch-organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Zutrittskontrolle: Die Zutrittskontrolle erfolgt über ein Zugangskontrollsystem des Subunternehmers (Anlage 2). Eine 24/7 Videoüberwachung sowie Einbruchmeldeanlage sind vorhanden.
- Zugangskontrolle**:** Individuelle Benutzeraccounts für den administrativen Zugriff auf das Managementsystem durch den Auftraggeber.
  Individuelle Benutzeraccounts für den Zugriff auf das bereitgestellte System werden durch den Kunden bereitgestellt.
  Kennwortkomplexität (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts,….) wird eingehalten.
  Automatische Sperrung (z.B. Kennwort Fehleingaben oder Pausenschaltung).
- Zugriffskontrolle: Differenzierte Berechtigungen im Management System (Profile, Rollen, Transaktionen und Objekte). Vergabe der Zugriffsrechte nach Prinzip der minimal erforderlichen Rechte.
- Trennungskontrolle: Durchgängige logische Trennung aller Mandanten in gekapselte Systeme und virtuelle Netzwerke. Unterschiedliche Datenbanken je Mandant.
- Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO) erfolgt im Ermessen und in Verantwortung des Auftraggebers.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- Weitergabekontrolle: Verschlüsselte Übertragung über SSL und IPSec geschützte Verbindungen.
- Eingabekontrolle: Protokollierungs- und Protokollauswertungssysteme

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Verfügbarkeitskontrolle
- Redundante Server
- Redundante Internetanbindung
- Spiegeln von Festplatten, RAID-Verfahren sowie Sicherung der Gesamtsysteme
- Unterbrechungsfreie Stromversorgung (USV) 1+n redundant
- Virenschutz / Firewall

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Datenschutz-Management;
- Incident-Response-Management;
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);
- Auftragskontrolle
  Eindeutige Vertragsgestaltung
  Formalisierte und dokumentierte Auftragserteilung (per eMail)
  Kontrolle der Vertragsausführung

Anlage 2 – Unterauftragsverhältnisse

Firma Unterauftragnehmer	Anschrift/Land	Leistung
KRK Computersysteme GmbH	Nienburger Straße 9a D-27232 Sulingen	Bereitstellung von Rechenzentrumsdienstleistungen (RZ der kyberio GmbH). Vertrag zur Auftragsverarbeitung ist abgeschlossen.