QUMsult
BERATUNG UND SOFTWARE

Vertrag zur Auftrags-verarbeitung gemäß Art. 28 DSGVO für die Anwendungen

WebSARA

EHS-Software mit den Modulen AwSV, Gefahrstoffe, Abfall und Gefährdungsbeurteilung, Anlage

PAUL §

Das Rechtsverzeichnis für Arbeitsschutz-, Energie- und Umweltrecht

UTA

Unterweisungen und Schulungen managen

KUMA

Interne Anwendung für das Kundenmanagement

QUMsult GmbH & Co. KG
Eisenbahnstraße 41
D-79098 Freiburg

Tel 07 61 / 2 92 86-10
E-Mail info@qumsult.de
Internet www.qumsult.de

1 Information zu Vertrag, Auftragnehmerin und Auftraggeber

Vorbemerkung:
Der Vertrag ist bereits digital unterzeichnet und in dieser Form gültig.
Bitte drucken Sie diesen aus, unterzeichnen Sie als „Auftraggeber“ und senden uns einen Scan per E-Mail an kunde@qumsult.de zurück. Erst dann gilt der Vertrag als abgeschlossen.

Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO zwischen der Firma

QUMsult GmbH & Co. KG

Eisenbahnstr. 41

79098 Freiburg

- nachfolgend **„Auftragnehmerin“** genannt -

und der Firma

Firmenname: _____

Straße, Hausnummer: _____

Postleitzahl, Ort: _____

- nachfolgend **„Auftraggeber“** genannt -

2 Präambel

Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus den Nutzungsbestimmungen ergeben. Sie findet Anwendung auf alle Tätigkeiten, die damit in Zusammenhang stehen und bei denen Beschäftigte der Auftragnehmerin oder durch die Auftragnehmerin Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Aus dem Vertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung. Im Einzelnen sind insbesondere die folgenden Daten Bestandteil der Datenverarbeitung:

Art der Daten	**Art und Zweck der Datenverarbeitung**	**Kategorien betroffener Personen**
Personenstammdaten	Konkretisierung und Zuordnung von Personen in Anwendungen (SaaS Online Dienste)	Bei Kunden: Beschäftigte des Kunden Bei Dienstleister: Dessen Kunden und Beschäftigte
Kommunikationsdaten	Zugangsverwaltung und Kommunikation	Bei Kunden: Beschäftigte des Kunden Bei Dienstleister: Dessen Kunden und Beschäftigte

Die Laufzeit des Vertrages richtet sich nach der Dauer der Erbringung von Online-Diensten (SaaS) der Auftragnehmerin an den Auftraggeber. Der Auftrag endet, wenn der Auftraggeber keine Online-Dienste der Auftragnehmerin, entsprechend den Leistungsvereinbarungen/Angeboten der einzelnen Auftragsbestätigungen von Online-Diensten der Auftragnehmerin, mehr in Anspruch nimmt.

§ 2 Anwendungsbereich und Verantwortlichkeit

1. Die Auftragnehmerin verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an die Auftragnehmerin sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DSGVO).
2. Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die von der Auftragnehmerin bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

§ 3 Pflichten der Auftragnehmerin

1. Die Auftragnehmerin darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DSGVO vor. Die Auftragnehmerin informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Ge-

setze verstößt. Die Auftragnehmerin darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

2. Die Auftragnehmerin wird in ihrem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz- Grundverordnung (Art. 32 DSGVO) genügen. Die Auftragnehmerin hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Die Aufragnehmerin hält ihre Systeme auf dem Stand der Technik und verbessert diese. (Genaueres siehe Anlage 1).
   Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt der Auftragnehmerin vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.
3. Die Auftragnehmerin unterstützt soweit vereinbart den Auftraggeber im Rahmen ihrer Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten.
4. Die Auftragnehmerin gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter/innen und andere für die Auftragnehmerin tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet die Auftragnehmerin, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.
5. Die Auftragnehmerin unterrichtet den Auftraggeber unverzüglich, wenn ihr Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden.
   Die Auftragnehmerin trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.
6. Die Auftragnehmerin nennt dem Auftraggeber den/die Ansprechpartner/in für im Rahmen des Vertrages anfallende Datenschutzfragen, siehe Anlage 1.
7. Die Auftragnehmerin gewährleistet, ihren Pflichten nach Art. 32 Abs. 1 lit. d) DSGVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.
8. Die Auftragnehmerin berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt die Auftragnehmerin die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart.
   In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe, Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart.
9. Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen.
   Im Falle von Test- und Ausschussmaterialien ist eine Einzelbeauftragung nicht erforderlich.

Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

10. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichtet sich die Auftragnehmerin den Auftraggeber bei der Abwehr des Anspruches im Rahmen ihrer Möglichkeiten zu unterstützen.
11. Sofern die Auftragnehmerin die Wartung und/oder Pflege der IT-Systeme auch im Wege der Fernwartung durchführt, ist die Auftragnehmerin verpflichtet, dem Auftraggeber eine wirksame Kontrolle der Fernwartungsarbeiten zu ermöglichen. Dies kann z.B. durch Einsatz einer Technologie erfolgen, die dem Auftraggeber ermöglicht, die von der Auftragnehmerin durchgeführten Arbeiten auf einem Monitor o.ä. Gerät zu verfolgen.
    Wenn der Auftraggeber bei Fernwartungsarbeiten nicht wünscht, die Tätigkeiten an einem Monitor o.ä. Gerät zu beobachten, wird die Auftragnehmerin die von ihr durchgeführten Arbeiten in geeigneter Weise dokumentieren.
12. Eine Verlagerung der Datenverarbeitung in Drittstaaten geschieht nur unter Feststellung eines angemessenen Schutzniveaus nach Art. 44 DSGVO und der Zustimmung des Auftraggebers. Die Auftragnehmerin stellt die für Feststellung eines angemessenen Schutzniveaus notwendigen Informationen zur Verfügung.
13. Die Auftragnehmerin verpflichtet sich dazu bei Anfragen der Aufsichtsbehörde mit dieser zusammenzuarbeiten.

§ 4 Pflichten des Auftraggebers

1. Der Auftraggeber hat die Auftragnehmerin unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
2. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, gilt §3 Abs. 10 entsprechend.
3. Der Auftraggeber nennt der Auftragnehmerin den/die Ansprechpartner/in für im Rahmen des Vertrages anfallende Datenschutzfragen.

§ 5 Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung Löschung oder Auskunft an die Auftragnehmerin, wird die Auftragnehmerin die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Die Auftragnehmerin leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Die Auftragnehmerin unterstützt den Auftraggeber im Rahmen ihrer Möglichkeiten auf Weisung. Die Auftragnehmerin haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird, es sei denn, die Auftragnehmerin hat dies zu vertreten.

§ 6 Nachweismöglichkeiten

1. Die Auftragnehmerin weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach. Dazu gehören Interne Audits im Rahmen des Zertifizierungsprozesses nach ISO 9001 und 14001.
2. Sollten im Einzelfall Inspektionen durch den Auftraggeber oder eine/n von diesem beauftragte/n Prüferin erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Die Auftragnehmerin darf diese von der vorherigen Anmel-

dung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen (Ausgenommen sind Berufsgeheimnisträger). Sollte der/die durch den Auftraggeber beauftragte Prüfer/in in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat die Auftragnehmerin gegen diesen ein Einspruchsrecht.

§ 7 Subunternehmen (weitere Auftragsverarbeiter/innen)

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 die Auftragnehmerin z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Die Auftragnehmerin 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 Einsatz von Subunternehmen als weiteren Auftragsverarbeiter/innen ist nur zulässig, wenn der Auftraggeber vorher zugestimmt hat.
3. Ein zustimmungspflichtiges Subunternehmensverhältnis liegt vor, wenn die Auftragnehmerin weitere Auftragnehmer/innen mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt. Die Auftragnehmerin wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.

   Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung folgender Subunternehmer durchgeführt:

Name und Anschrift des Subunternehmens	**Beschreibung der Teilleistungen**
Host Europe GmbH Hansestrasse 111 51149 Köln	Server-Hosting
netcup GmbH Daimlerstraße 25 D-76185 Karlsruhe	Server-Hosting
manitu GmbH Welvertstraße 2 66606 St. Wendel	Domain Bereitstellung und E-Mail Server
VISUS IT Darmstädter Str. 51 B 64404 Bickenbach	Programmierdienstleistungen nur den Online-Dienst Paul betreffend
Continum AG Bismarckallee 7b-7d 79098 Freiburg im Breisgau	Managed Cloud Service

   Vor der Hinzuziehung weiterer oder der Ersetzung aufgeführter Subunternehmen holt die Auftragnehmerin die Zustimmung des Auftraggebers ein, wobei diese nicht ohne wichtigen datenschutzrechtlichen Grund verweigert werden darf.
4. Erteilt die Auftragnehmerin Aufträge an Subunternehmen, so obliegt es der Auftragnehmerin, ihre datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmen zu übertragen.

§ 8 Informationspflichten, Schriftformklausel, Rechtswahl

1. Sollten die Daten des Auftraggebers bei der Auftragnehmerin durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat die Auftragnehmerin den Auftraggeber unverzüglich darüber zu informieren. Die Auftragnehmerin wird alle in diesem Zusammenhang Verantwortliche unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher« im Sinne der Datenschutz-Grundverordnung liegen.
2. Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen der Auftragnehmerin – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
3. Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.
4. Es gilt deutsches Recht.

§ 9 Haftung und Schadensersatz

Auftraggeber und Auftragnehmerin haften gegenüber betroffener Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

§ 10 Salvatorische Klausel, Gerichtsstand

1. Sollte eine Bestimmung dieses Vertrages ungültig oder undurchsetzbar sein oder werden, so bleiben die übrigen Bestimmungen dieses Vertrages hiervon unberührt. Die Parteien vereinbaren, die ungültige oder undurchsetzbare Bestimmung durch eine gültige und durchsetzbare Bestimmung zu ersetzen, welche wirtschaftlich der Zielsetzung der Parteien am nächsten kommt. Das Gleiche gilt im Falle einer Regelungslücke.
2. Als Gerichtsstand wird Freiburg vereinbart.

_____, den _____

_____

Auftraggeber

_____

i.V. der Auftragnehmerin

QUMsult GmbH & Co. KG
Eisenbahnstr. 41
D-79098 Freiburg i. Br.
Tel. 0761-2 92 86-10
Fax 0761-2 92 86-77

Ansprechpartner für Datenschutzfragen:

Dominik Bährle – baehrle@qumsult.de

Anlage 1 – Technische-organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Zutrittskontrolle
  Kein unbefugter Zutritt zu Datenverarbeitungsanlagen:
  Schlüssel / Schlüsselvergabe
- Zugangskontrolle
  Keine unbefugte Systembenutzung:
  Kennwortverfahren (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts)
  Einrichtung eines Benutzerstammsatzes pro User
- Zugriffskontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems:
  Differenzierte Berechtigungen (Profile, Rollen, Transaktionen und Objekte)
- Trennungskontrolle
  Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden.
  Sowie einzelne Datenbanken für unterschiedliche Daten und Kunden.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

- Weitergabekontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport:
  Verschlüsselung (HTTPS, SSL – SHA256), Protokollierung
- Eingabekontrolle
  Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:
  Protokollierung, Dokumentenmanagement

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Verfügbarkeitskontrolle
  Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust:
  Backup-Strategie, unterbrechungsfreie Stromversorgung (USV)
  Virenschutz, Firewall
  Meldewege und Notfallpläne
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)
- Standort der unternehmenseigenen Server und des Rechenzentrums befinden sich in Deutschland und / oder einem Mitgliedsstaat oder ggf. auch mehreren Mitgliedsstaaten der EU

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

- Datenschutz-Management
- Incident-Response-Management
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)
- Auftragskontrolle
  Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.