HKM Consulting GmbH

Systematik und Aufbau der Compliance-konformen Dokumentenarchitektur

Erläuternde Übersicht zur Dokumentenstruktur und Verzahnung der AGB mit den Managementsystemen der HKM Consulting GmbH

Version 1.14 | Stand: Februar 2025

Amtsgericht München – HRB 209780
Sitz: 85521 Hohenbrunn / Metropolregion München
Gerichtsstand: München (Deutschland)
www.hkm-consulting.de | info@hkm-consulting.de | Tel. +49 89 31699-505

Präambel und Dokumentenstruktur

Systematik und Aufbau der Compliance-konformen Dokumentenarchitektur

Die HKM Consulting GmbH betreibt ein integriertes Managementsystem, das die Bereiche **Qualitätsmanagement (QMS)**, **Informationssicherheits-Management (ISMS)**, **IT-Service-Management (ITSM)**, **Datenschutzmanagement (DSMS)**, **Umwelt- und Nachhaltigkeitsmanagement (UMS)**, **Künstliche Intelligenz-Management (AIMS)** sowie die **technisch-organisatorischen Maßnahmen (TOMs)** in einer durchgängigen Governance-Struktur vereint.

Dieses System stellt sicher, dass alle rechtlichen, technischen und organisatorischen Verpflichtungen miteinander abgestimmt sind und den Anforderungen aus nationalem und europäischem Recht entsprechen.

Im Zentrum dieser Struktur stehen die **Allgemeinen Geschäftsbedingungen (AGB)** der HKM Consulting GmbH.
Sie definieren die juristische und organisatorische Grundlage sämtlicher Geschäfts- und Leistungsbeziehungen.

Um Konsistenz, Nachvollziehbarkeit und Auditfähigkeit sicherzustellen, sind die AGB inhaltlich und sprachlich mit allen nachfolgenden Dokumenten und Managementsystem-Elementen verknüpft.

Die einzelnen Bestandteile dieses integrierten Dokumentensystems sind:

- **Leistungsbeschreibung / Statement of Work (SoW)**

  Beschreibung mit Bezug zur AGB
  Die SoW-Dokumente konkretisieren die in den AGB definierten Leistungsarten und dienen als operative Umsetzungsebene. Sie sind vollständig in das Qualitätsmanagementsystem (QMS) und die Prozesslandkarte integriert und bilden dort den verbindlichen Ablauf der Projektplanung, Leistungserbringung und Abnahme ab.
  Sie stellen die operative Ausgestaltung der in § 3 AGB genannten Leistungspflichten dar und dienen als messbare Grundlage für Projektumfang, Abnahmebedingungen und Mitwirkungspflichten.

  Bezug zu System und Norm
  Bestandteil des **QMS gemäß ISO 9001:2015** und im **Business Process Management System (BPMS)** abgebildet. Gewährleistet nachvollziehbare Dokumentation von Anforderungen, Liefergegenständen und Ergebnissen entlang der Prozesslandkarte.

- **Service Level Agreement (SLA)**

  Beschreibung mit Bezug zur AGB
  Das SLA ist Bestandteil des Informationssicherheits- und IT-Service-Managementsystems (ISMS / ITSM).
  Es regelt Reaktions- und Wiederherstellungszeiten, Eskalationsmechanismen sowie Servicefenster und stellt sicher, dass alle in den AGB beschriebenen Leistungspflichten technisch und organisatorisch hinterlegt sind.
  Es konkretisiert die Verpflichtungen aus § 9 AGB („Betrieb, Support und Wartung“) und definiert die operativen Leistungsparameter, die für Vertragserfüllung und Nachweisführung maßgeblich sind.

  Bezug zu System und Norm
  Das **ITSM nach ISO 20000-1:2015** legt Prozesse, Rollen und Verfahren zur Planung, Bereitstellung und Verbesserung von IT-Dienstleistungen fest.
  Über Schnittstellen zum ISMS wird die Einhaltung von Verfügbarkeits-, Sicherheits- und Qualitätskennzahlen sichergestellt.

- **Auftragsverarbeitungsvertrag (AVV)**

  Beschreibung mit Bezug zur AGB
  Der AVV ist vollständig in das Datenschutzmanagementsystem (DSMS) und die TOMs eingebettet.
  Er dokumentiert datenschutzrechtliche Rollen, Verantwortlichkeiten und Schutzmaßnahmen und gewährleistet die Übereinstimmung mit den AGB-Bestimmungen zu Datenschutz und Vertraulichkeit.
  Ergänzt § 11 AGB („Datenschutz“) und beschreibt die datenschutzrechtliche Umsetzung der Vertragsbeziehung zwischen Verantwortlichem und Auftragsverarbeiter.

  Bezug zu System und Norm
  Das **DSMS** basiert auf der **DSGVO / GDPR** und ist mit dem **ISMS** sowie den **TOMs gemäß Art. 32 DSGVO** verbunden.
  Der AVV dokumentiert die Integration organisatorischer und technischer Schutzmaßnahmen.

- **Lösch- und Aufbewahrungskonzept**

  Beschreibung mit Bezug zur AGB
  Dieses Konzept ist Teil des Datenschutz- und Informationssicherheitsmanagements und beschreibt die technische und organisatorische Umsetzung von Lösch-, Archivierungs- und Aufbewahrungsprozessen nach Art. 17 und 32 DSGVO.
  Es ist prozessual mit dem QMS verknüpft, um eine revisionssichere Datenverwaltung sicherzustellen.
  Es konkretisiert die AGB-Regelungen zu Datenschutz und Vertraulichkeit und schafft eine überprüfbare Grundlage für Datenlöschung, Aufbewahrung und Nachweisführung.

  Bezug zu System und Norm
  Bestandteil des **DSMS** und **ISMS**, auf Basis von **ISO 27001**, **BSI-200-Reihe** und **DSGVO**.
  Dient der nachvollziehbaren und rechtssicheren Handhabung personenbezogener Daten.

- **Sicherheits- und Compliance-Anforderungen (Security Annex)**

  Beschreibung mit Bezug zur AGB
  Der Security Annex konkretisiert die Sicherheits- und Compliance-Vorgaben aus den AGB.
  Er basiert auf dem ISMS und berücksichtigt die Anforderungen aus ISO 27001, NIS-2 und dem EU Cyber Resilience Act.
  Durch Anbindung an Risikomanagement und QMS wird sichergestellt, dass Sicherheitsmaßnahmen nicht nur dokumentiert, sondern auch prozessual verankert sind.
  Umsetzung von § 12 AGB („Informationssicherheit und Compliance“).

  Bezug zu System und Norm
  Stützt sich auf **ISMS**, **ITSM** und **AIMS**.
  Verweist auf **ISO/IEC 27001:2018**, **BSI 200-1 bis 200-4**, **NIS-2 (EU 2022/2555)** und **CRA (EU 2024/2847)**.

- **Incident-Response- und Business-Continuity-Konzepte**

  Beschreibung mit Bezug zur AGB
  Operative Bestandteile des ISMS und ITSM.
  Sie gewährleisten, dass die in den AGB geregelten Melde-, Reaktions- und Wiederherstellungsverpflichtungen technisch abgebildet und regelmäßig getestet werden.
  Umsetzung von § 12 Abs. 2 AGB („Sicherheitsvorfälle“).

  Bezug zu System und Norm
  Nach **ISO 27001**, **BSI 200-4** und den Prozessanforderungen des ITSM.
  Zentrales Instrument für Krisen-, Notfall- und Wiederanlaufmanagement.

- **Lizenzbedingungen und Open-Source-Notices (OSS-Notices)**

  Beschreibung mit Bezug zur AGB
  In die Qualitäts- und Entwicklungsprozesse des QMS integriert.
  Dokumentieren Nutzungsrechte und Lizenzverpflichtungen für eingesetzte Softwarekomponenten und gewährleisten die rechtssichere Umsetzung von § 8 AGB („Urheberrechte, Lizenzen“).

  Bezug zu System und Norm
  Basieren auf **QMS (ISO 9001:2015)** und **ISMS (ISO 27001:2018)**.
  Sichern durch standardisierte Prüfungen die rechtliche und sicherheitstechnische Integrität von Software-Elementen.

- **Exit- und Übergabekonzept**

  Beschreibung mit Bezug zur AGB
  Bestandteil der Prozesse „Vertragsbeendigung“ und „Datenrückgabe“ im QMS, ISMS und DSMS.
  Beschreibt Abläufe zur sicheren Übergabe oder Löschung von Daten und Systemzugängen bei Vertragsende und operationalisiert § 15 AGB.

  Bezug zu System und Norm
  Nach **ISO 9001**, **ISO 27001** und **DSGVO**.
  Integriert Datenschutz, Informationssicherheit und Prozesssteuerung in die Abwicklungsphase.

- **Künstliche Intelligenz-Management (AIMS)**

  Beschreibung mit Bezug zur AGB
  Ergänzt die bestehenden Regelungen der AGB um KI-bezogene Aspekte von Transparenz, Sicherheit und ethischer Verantwortung.
  Konkretisierung der Compliance-Verpflichtungen aus § 12 AGB und Sicherstellung, dass KI-gestützte Systeme verantwortungsvoll betrieben werden.

  Bezug zu System und Norm
  Nach **ISO/IEC 42001:2023**.
  Eng verknüpft mit **ISMS**, **QMS**, **DSMS** und **Risikomanagement**.
  Ergänzt den Security Annex um KI-spezifische Kontrollprozesse.

- **Interne Richtlinien und Policies**

  Beschreibung mit Bezug zur AGB
  Richtlinien zu Compliance, Data Classification, Access Control, Nachhaltigkeit und Umweltmanagement sind integrale Bestandteile der jeweiligen Managementsysteme (QMS, ISMS, UMS, DSMS, AIMS).
  Sie gewährleisten die interne Umsetzung der in den AGB verankerten Grundsätze und konkretisieren § 2 AGB („Grundsätze und Geltung der Bedingungen“).

  Bezug zu System und Norm
  Basieren auf **ISO 9001**, **ISO 27001**, **ISO 14001**, **ISO 20000-1** und **ISO/IEC 42001**.
  Bilden das verbindliche interne Regelwerk für Compliance, Prozesssteuerung und Nachhaltigkeit.

Durch diese durchgängige Integration ist das Dokumentensystem der HKM Consulting GmbH in der Lage, rechtliche, organisatorische und technische Anforderungen vollständig und konsistent abzubilden.
Die AGB fungieren dabei als verbindendes Regelwerk zwischen Managementsystemen, operativen Prozessen und Kundenvereinbarungen.
Diese Struktur schafft Transparenz, Prüfbarkeit und Vertrauen – sowohl im Rahmen interner Audits als auch gegenüber Kunden und Aufsichtsbehörden.