

Leistungsbeschreibung

Vergabe-Nr. 1335-0126

Ausschreibung über den Betrieb, das Hosting und die Weiterentwicklung der Website www.kkh.de inklusive Migration auf ein zukunftsfähiges CMS-System



**Kaufmännische Krankenkasse - KKH
Karl-Wiechert-Allee 61
30625 Hannover**

Inhaltsverzeichnis

I. Glossar.....	5
II. Leistungsbeschreibung	10
1. Ausgangslage	10
2. Ziel der Beschaffung	10
3. Gegenstand der Ausschreibung.....	11
3.1 Leistungsumfang	11
3.2 Leistungszeitraum	11
3.3 Leistungsabnahme	13
3.4 Feinkonzeption & Entwicklungsprozess.....	13
3.5 Kooperation mit dem Bestandsdienstleister.....	14
3.6 Befähigung & Systemeinführung	14
3.7 Vertragslaufzeit und Vergütung	14
3.8 Ablaufplan	15
4. Anforderungen	15
4.1 Anforderungen an den Auftragnehmer.....	15
4.1.1 Leistungsfähigkeit und Kompetenzprofil	15
4.1.2 Personalausstattung: Qualifikationsprofile	15
4.1.3 Wissenstransfer und Projektsicherheit.....	22
4.1.4 Referenzen und Branchenerfahrung	23
4.1.5 Interessenkonflikte	23
4.1.6 Versicherungssummen.....	23
4.2 Anforderungen an Vorgehensmodell und Projektorganisation	23
4.2.1 Vorgehensmodell	23
4.2.2 Anforderungsmanagement	24
4.2.3 Beauftragung von Einzelaufträgen	24
4.2.4 Toolset und Kommunikation	24
4.2.5 Projektstart und Zusammenarbeit.....	25
4.3 Anforderungen an das CMS	26
4.3.1 Systemauswahl und Empfehlung	26
4.3.2 Lizenzmodell und Kosten	26
4.3.3 Rollen- und Rechtemanagement.....	27
4.3.4 Content-Pflege und Redaktionsfunktionen	27

4.3.5 Komponenten, Templates und Containerlösung.....	28
4.3.6 Medien- und Asset-Management.....	28
4.3.7 Mehrsprachigkeit.....	29
4.3.8 Inhaltsmodelle und Flexibilität	29
4.3.9 Suchfunktion	30
4.3.10 Schnittstellenintegration	30
4.3.11 Online-Rechner	31
4.3.12 Online-Formulare, Online-Beitrittserklärung und E-Mail-Routing	33
4.3.13 Öffentliche Zustellung.....	36
4.3.14 Weiterführende CMS-Funktionen	37
4.4 Anforderungen an Betrieb und technische Architektur.....	37
4.4.1 Zielarchitektur.....	37
4.4.2 Umgebungskonzept	38
4.4.3 Deployment-Prozess	38
4.4.4 Monitoring, Logging und Alerting	39
4.4.5 Zertifikate	39
4.5 Anforderungen an Content-Migration.....	40
4.6 Anforderungen an Barrierefreiheit und Nutzerorientierung.....	40
4.6.1 Anforderungen an Barrierefreiheit	40
4.6.2 Barrierefreiheit im laufenden Betrieb	41
4.6.3 Mobile-First	41
4.7 Anforderungen an IT-Sicherheit und Datenschutz	42
4.7.1 Compliance mit KKH Security-Guide für digitale Services	42
4.7.2 Löschkonzept und Aufbewahrungsfristen	42
4.7.3 Datenspeicherung und -verarbeitung	43
4.7.4 Wartung/Support/Service etc.....	43
4.7.5 Schutzbedarfs- und KRITIS-Scope-Bewertung.....	44
4.7.6 Risikoanalyse	44
4.7.7 Audit-, Kontroll- und Nachweisrechte.....	44
4.8 Anforderungen an SEO und Generative Engine Optimization (GEO/LLMO).....	44
4.8.1 Technische SEO-Grundlage (Crawling & Indexierung).....	44
4.8.2 On-Page-SEO und Metadaten	45
4.8.3 URL-Struktur, Weiterleitungen und Systemseiten.....	45
4.8.4 SEO-sicherer Relaunch.....	46

4.8.6 Analytics, Tracking und Search Console	46
4.8.7 Optimierung für KI-gestützte Systeme (LLMO/GEO)	47
4.8.8 Erweiterte SEO-Funktionen (Optional)	47
4.9 Anforderungen an Zukunftsfähigkeit und Innovation	48
4.9.1 Integration neuer Technologien	48
5. Leistungsort/Lieferbedingungen	48
6. Schulungsangebote	49
7. Dokumentation und Übergabe bei Vertragsende	50

I. Glossar

Begriff	Beschreibung/Erläuterung
AI Act (EU AI Act)	Europäische Verordnung zur Regulierung von KI-Systemen. Sie legt risikobasierte Anforderungen fest, u. a. an Klassifizierung, Dokumentation, menschliche Aufsicht und KI-Kompetenz.
API	Application Programming Interface: Anwendungsprogrammierschnittstelle
BITV 2.0	Barrierefreie-Informationstechnik-Verordnung: Eine deutsche Rechtsverordnung, die regelt, wie digitale Angebote des Bundes für Menschen mit Behinderungen zugänglich sein müssen. Sie setzt das Behindertengleichstellungsgesetz um und sorgt dafür, dass Websites, Apps und Software ohne fremde Hilfe nutzbar sind.
BCM	Business Continuity Management: Systematisches Notfall - und Kontinuitätsmanagement. Ziel ist, kritische Geschäftsprozesse und IT -Services auch bei Störungen, Cyberangriffen oder Ausfällen in einem definierten Mindestumfang weiterzuführen bzw. schnell wiederherzustellen.
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik. Es regelt u. a. Risikomanagement, Angriffserkennung, Meldepflichten und Nachweisprüfungen für Betreiber kritischer Infrastrukturen.
B3S-GKV/PV	Branchenspezifischer Sicherheitsstandard für die gesetzliche Kranken- und Pflegeversicherung. Er konkretisiert die Anforderungen an die IT-Sicherheit kritischer

	Infrastrukturen in diesem Sektor und wurde vom BSI festgestellt.
Chain of Custody	Lückenlos dokumentierte Beweiskette, die belegt, wer wann Zugriff auf digitale Beweismittel hatte und dass diese unverändert geblieben sind.
CI/CD-Pipeline	Automatisierter Arbeitsablauf in der Softwareentwicklung, der die Schritte Continuous Integration (CI), Continuous Delivery (CD) und Continuous Deployment (CD) verbindet, um Code von der Idee bis in die Produktion zu bringen
CMS	Content Management System
CRA	Cyber Resilience Act: Europäische Verordnung mit Cybersicherheitsanforderungen an Produkte mit digitalen Elementen, u. a. zu Schwachstellenmanagement, Sicherheitsupdates und Herstellersupport.
CVE	Common Vulnerabilities and Exposures: Standardisierte Kennung für öffentlich bekannte Sicherheitslücken in Soft- und Hardware.
C5-Testat Typ 2	Prüfnachweis nach dem Kriterienkatalog „Cloud Computing Compliance Criteria Catalogue“ des BSI. Ein Typ-2-Testat bestätigt zusätzlich die Wirksamkeit der Sicherheitsmaßnahmen über einen Zeitraum. Für Cloud-Dienste mit Sozial- und Gesundheitsdaten nach § 393 SGB V erforderlich.
DAM	Digital Asset Management
DAST	Dynamic Application Security Testing: Sicherheitstest einer laufenden Anwendung von außen, um Schwachstellen aufzudecken.
Deployment	Bereitstellung und Veröffentlichung

DSGVO	Datenschutz-Grundverordnung: Ein einheitliches EU-Gesetz, das den Schutz personenbezogener Daten, die Rechte von Verbrauchern und die Pflichten von Unternehmen regelt. Sie gilt seit dem 25. Mai 2018 in allen Ländern der Europäischen Union.
EOL/EOS	End of Life / End of Support: Zeitpunkt, ab dem ein Produkt nicht mehr weiterentwickelt bzw. nicht mehr mit Sicherheitsupdates versorgt wird.
GEO	Generative Engine Optimization: Optimierung für generative Suchsysteme
IoC	Indicator of Compromise: Technisches Merkmal (z. B. Dateihash, IP-Adresse, Log-Muster), das auf einen Sicherheitsvorfall hindeutet.
JIT	Just-in-Time-Zugriff: Befristete Vergabe erhöhter Rechte nur bei Bedarf.
KRITIS	Kritische Infrastruktur: Einrichtung von hoher Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten (z. B. das Gesundheitswesen).
Least Privilege	Prinzip der minimalen Rechtevergabe: Nutzer und Systeme erhalten nur die Rechte, die sie für ihre Aufgabe zwingend benötigen.
LLMO	Large Language Model Optimization: Optimierung für große Sprachmodelle
MFA	Multi-Faktor-Authentifizierung: Anmeldung mit mindestens zwei unabhängigen Nachweisen (z. B. Passwort und Einmalcode).

PAM	Privileged Access Management: Verwaltung, Absicherung und Protokollierung privilegierter Zugriffe.
Redesign	Neugestaltung/Umgestaltung
RPO	Recovery Point Objective: Maximal akzeptabler Datenverlust, ausgedrückt als Zeitspanne. Beispiel: RPO = 1 Stunde bedeutet, dass im Störfall höchstens die Daten der letzten Stunde verloren gehen dürfen.
RTO	Recovery Time Objective: Maximal zulässige Zeitspanne, innerhalb derer ein ausgefallener Service nach einer Störung wieder verfügbar sein muss. Beispiel: RTO = 4 Stunden bedeutet, dass der Service spätestens nach vier Stunden wiederhergestellt sein soll.
SAST	Static Application Security Testing: Analyse des Quellcodes auf Sicherheitslücken, ohne die Anwendung auszuführen.
SBOM	Software Bill of Materials: Vollständige Stückliste aller in einer Software enthaltenen Komponenten und Abhängigkeiten.
SGB V	Fünftes Buch Sozialgesetzbuch – Gesetzliche Krankenversicherung: Regelt die medizinische Versorgung, Prävention, Krankheitsbehandlung, Zahnheilkunde sowie Leistungen bei Schwangerschaft und Mutterschaft.
SGB X	Zehntes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz: Regelt das einheitliche sozialrechtliche Verwaltungsverfahren, den Sozialdatenschutz sowie die Zusammenarbeit der Sozialleistungsträger in Deutschland.
SEO	Search Engine Optimization: Suchmaschinenoptimierung

SIEM	Security Information and Event Management: System zur zentralen Erfassung und Auswertung sicherheitsrelevanter Logdaten.
SLA	Service-Level-Agreement: Schriftliche Vereinbarung zwischen einem Auftragnehmer und einem Kunden, die genaue Qualitätsstandards, Reaktionszeiten und die Verfügbarkeit von Leistung festlegen
SOC	Security Operations Center: Stelle zur kontinuierlichen Überwachung und Bewertung von Sicherheitsereignissen.
Sozialdaten	Personenbezogene Daten, die von einem Sozialleistungsträger (z. B. der KKH) zur Erfüllung seiner Aufgaben verarbeitet werden (§ 67 SGB X). Sie unterliegen dem Sozialgeheimnis.
TDDDG	Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz: Regelt u. a. in § 25 den Zugriff auf Endgeräte und den Einsatz von Cookies und Tracking, die eine wirksame Einwilligung erfordern.
URL	Uniform Resource Locator: Internetadresse/Webadresse
UX-Design	User Experience-Design: Kümmert sich um das gesamte Erlebnis und die einfache Bedienung eines Produkts.
UI-Design	User Interface-Design: Gestaltet das Aussehen und die Benutzeroberfläche eines digitalen Produkts. Sorgt im Zusammenspiel mit UX-Design für funktionale sowie ansprechende Apps oder Websites.
WAF	Web Application Firewall: Schutzsystem, das Webanwendungen vor typischen Angriffen wie Injection oder Cross-Site-Scripting abschirmt

WCAG 2.2 AA	Web Content Accessibility Guidelines, Version 2.2, Stufe AA: Ein internationaler Standard für barrierefreies Webdesign. Die Stufe AA gilt weltweit sowie in der EU als der wichtigste, rechtlich verbindliche Mindeststandard, um digitale Angebote für Menschen mit Behinderungen zugänglich zu machen.
WYSIWYG-Editor	What You See Is What You Get (Deutsch: Was du siehst, ist das, was du bekommst) Editor: Ein Software-Programm, mit dem man digitale Inhalte direkt so bearbeiten kann, wie sie später auch aussehen werden

II. Leistungsbeschreibung

1. Ausgangslage

Die Kaufmännische Krankenkasse (KKH) beabsichtigt die technische und konzeptionelle Neuausrichtung ihrer Website www.kkh.de. Zentraler Bestandteil des Projekts ist die Migration des bestehenden Content-Management-Systems Adobe Experience Manager (AEM) auf eine moderne, zukunftssichere CMS-Plattform. In den Projektumfang eingeschlossen ist zudem das unter einer eigenen Subdomain betriebene Angebot „Arztlotse“ (arztlotse.kkh.de), das in dieselbe neue Systemumgebung zu überführen ist.

2. Ziel der Beschaffung

Ziel ist eine inhaltlich weitgehend deckungsgleiche, zugleich aber technisch und redaktionell professionalisierte Umsetzung der Website www.kkh.de. Funktionale, strukturelle und gestalterische Elemente der bestehenden Seite sind zu berücksichtigen, Informationsverluste hingegen sind zu vermeiden. Abweichungen von der bestehenden Struktur sind zulässig und mit der KKH abzustimmen, sofern sie der Verbesserung von Nutzerführung, Wartbarkeit oder technischer Qualität dienen. Das visuelle Erscheinungsbild basiert auf der aktuellen Web-Guideline der KKH und ist verbindlich einzuhalten. Ein umfassendes Redesign ist nicht Bestandteil dieses Vorhabens.

Der beauftragte Auftragnehmer soll nach erfolgreicher Migration kontinuierlich beim Ausbau, der Optimierung und der Weiterentwicklung der digitalen Plattform unterstützen.

Das Projektziel ist eine skalierbare, wartungsfreundliche und zukunftssichere Systemlandschaft, die den wachsenden Anforderungen der KKH gerecht wird und eine flexible Weiterentwicklung ermöglicht. Dabei sind gesetzlichen Anforderungen an Datenschutz, IT-Sicherheit und Barrierefreiheit vollständig einzuhalten.

3. Gegenstand der Ausschreibung

3.1 Leistungsumfang

Gegenstand dieser Ausschreibung ist die Beauftragung eines Full-Stack-Auftragnehmers mit folgendem Leistungsumfang:

- Migration von www.kkh.de sowie arztlotse.kkh.de vom bestehenden CMS (Adobe Experience Manager) auf eine neue, moderne CMS-Plattform
- Konzeption, Entwicklung und Implementierung des neuen Systems einschließlich CMS, Frontend, Schnittstellen und Betriebsinfrastruktur
- Vollständige Content-Migration inklusive Redirect-Mapping
- Sicherstellung von Barrierefreiheit (BITV 2.0/WCAG 2.2 AA), Datenschutz (DSGVO/Sozialdatenschutz), SGB V und SGB X, KRITIS- Konformität (BSI-Standards) sowie IT-Sicherheit (BSI-Standards)
- SEO- und GEO/LLMO-Optimierung
- Betrieb, Hosting und technischer Support der Plattform
- Kontinuierliche Weiterentwicklung, Wartung im laufenden Betrieb
- Schulungen für Mitarbeiter des Auftraggebers (insbesondere das Team Digitales Content Management der KKH)

Die detaillierten Anforderungen an den Auftragnehmer, das CMS, den Betrieb sowie an Qualität, Rechtskonformität und Innovationsfähigkeit sind in Abschnitt 4 „Anforderungen“ beschrieben.

3.2 Leistungszeitraum

Der Vertrag beginnt mit Zuschlagserteilung. Mit Zuschlagserteilung wird unmittelbar, ohne weiteren Einzelauftrag, die Position Relaunch inkl. Feinkonzept beauftragt und entsprechend dem Preisblatt mit Abnahme vergütet. Nach Zuschlagserteilung startet der Leistungsabruf mit einem gemeinsamen Workshop zur Feinkonzeption im Haus der KKH-Hauptverwaltung in Hannover. Der Auftragnehmer und Auftraggeber stimmen einen gemeinsamen Termin ab. In diesem Workshop wird zwischen Auftragnehmer und Auftraggeber ein verbindlicher Zeitplan erarbeitet, aus dem hervorgeht, welche Vorbereitungen für den Relaunch (Migration und Go-Live von www.kkh.de sowie arztlotse.kkh.de) bis zum Go-Live umgesetzt werden können.

Für die Umsetzung der erforderlichen Vorbereitungen steht nach dem Workshop ein Zeitfenster von maximal sechs Monaten bis zur Inbetriebnahme bzw. zum Go-Live zur Verfügung. Vor dem Go-Live hat eine Abnahme durch den Auftraggeber zu erfolgen.

Nach aktuellem Planungsstand soll der Go-Live spätestens zum 27.08.2027 erfolgen.

Sollte sich im Rahmen des Workshops ergeben, dass der Go-Live bis zum 27.08.2027 nicht realisiert werden kann, werden die erforderlichen Vorbereitungsmaßnahmen entsprechend dem abgestimmten Zeitplan fortgeführt. In diesem Fall verschiebt sich der Go-Live-Termin auf den 27.02.2028.

Der Leistungsbeginn und die Vergütung für die Haupttätigkeit des Vertrags, welche die laufenden Kosten für die Bereitstellung der Plattform, den laufenden Betrieb sowie die Wartung umfasst, startet erst nach erfolgreichem Go-Live.

Bis zu diesem Zeitpunkt umfasst der Leistungsabruf ausschließlich die im Rahmen der Vorbereitungs- und Feinkonzeptionsphase erforderlichen Leistungen.

Vor dem Go-Live sind folgende vorbereitenden Punkte abzuschließen:

- **Setup & Infrastruktur:** Bereitstellung und Grundeinrichtung der Cloud-Betriebs- und Hosting-Umgebung inkl. CI/CD-Pipelines und Sicherheitsarchitektur
- **CMS-Setup:** Installation, Konfiguration und Grundeinrichtung des Content Management Systems (CMS) sowie aller Kernkomponenten und Schnittstellen
- **Feinkonzept und Technische Frontend-Spezifikation:** Erstellung und Abstimmung des technischen/fachlichen Feinkonzept inklusive der Übernahme der bestehenden Design-Vorgaben in eine technische Frontend-Komponentenbibliothek (UI/UX Component Library)
- **Agile Umsetzung:** Technische Realisierung der fachlichen Anforderungen, Custom Components und Integrationen in iterativen Sprints
- **Automatisierte Content-Migration & Schnittstellen:** Konzeption, technische Anbindung an das Altsystem (in Kooperation mit dem Bestandsdienstleister), Entwicklung und Durchführung der automatisierten Inhalts- und Medienmigration inkl. 301-Redirect-Mapping
- **Service & Support Management:** Anbindung und Inbetriebnahme des Helpdesk-/Ticketsystems für den laufenden Betrieb und Support
- **Schulung:** Einweisung des KKH-Redaktionsteams im bereits befüllten und voll funktionsfähigen Demosystem
- **Barrierefreiheit:** Einhaltung der gesetzlichen Vorgaben zur Barrierefreiheit (BITV 2.0/WCAG 2.2 AA Audits) inkl. geeignete Testberichte
- **Dokumentation:** Bereitstellung einer vollständigen System- und Betriebs-Dokumentation

Nach erfolgreichem Abschluss dieser Vorbereitungspunkte erfolgt der Go-Live und Cutover: Abstimmung des Cutover-Szenarios (unter Einbindung des Bestandsdienstleisters), Umstellung der Domainverwaltung/DNS und finale Produktivsetzung.

Der Leistungsbeginn für die Haupttätigkeit des Vertrags (Bereitstellung der Plattform, laufender Betrieb, Wartung) startet erst nach erfolgreichem Go-Live.

3.3 Leistungsabnahme

Die Leistung gilt als erbracht, wenn durch die beschriebenen Konzepte, Verfahren und Installationen die Grundlagen für einen produktionsfähigen Betrieb von www.kkh.de gelegt sind. Dies bedeutet im Einzelnen:

- Umzug aller Domains und Zertifikate zum Auftragnehmer vollzogen ist,
- alle Komponenten wie vertraglich festgelegt installiert und angepasst sind,
- Test und Qualitätssicherung aller fachlichen Anforderungen durch die KKH durchgeführt worden sind,
- die vertraglich vereinbarten nicht-funktionalen Anforderungen nachgewiesen sind,
- alle Dokumentationen zu den Produkten, Systemeinstellungen und Anpassungen erstellt und an die KKH übergeben wurden,
- ein dokumentierter Security- und Compliance-Abnahmenachweis gegen B3S-GKV/PV, BSIG, DSGVO, SGB V/X, ISO/IEC 27001/27002, BSI 200-x und CIS Controls v8.1 vorliegt,
- die Einweisung der KKH-Mitarbeiter vollzogen wurde, sodass sie alle Tätigkeiten eigenständig durchführen können,
- die KKH durch die Abnahme und Freigabe die Leistungserbringung bestätigt hat.

3.4 Feinkonzeption & Entwicklungsprozess

Direkt im Anschluss an die Grundeinrichtung der Arbeitsumgebungen erstellt der Auftragnehmer ein detailliertes Feinkonzept. Dieses umfasst die Architektur-, Komponenten- und Datenmodellbeschreibung. Parallel hierzu laufen der Aufbau der Hosting-Infrastruktur sowie die Bereitstellung der Umgebungen (Entwicklung, Staging, Produktion).

Die Realisierung der fachlichen Anforderungen erfolgt nach einem agilen oder hybriden Vorgehensmodell (z. B. Scrum/Kanban) mit zweiwöchigen Sprint-Zyklen, um Fortschritte kontinuierlich zu überprüfen und Risiken frühzeitig zu minimieren.

Die Migration aller bestehenden Webinhalte (Texte, Metadaten wie Meta-Titles/Description und Alt-Texte, Strukturdaten, Dokumente, Bild- und Medienbestände) erfolgt vollständig automatisiert bzw. skriptgestützt durch den Auftragnehmer. Eine manuelle Neuerstellung oder händische Neueingabe durch KKH-Mitarbeitende ist für den Altbestand explizit nicht vorgesehen.

Der Auftragnehmer entwickelt im Rahmen des Feinkonzepts einen detaillierten Migrationsplan sowie entsprechende Import-Skripte /Schnittstellen (APIs). Die Inhaltsstruktur inklusive aller zugehörigen Metadaten wird vom Auftragnehmer aus dem Bestandssystem ausgelesen, semantisch bereinigt (HTML-Cleansing) und automatisiert in das neue CMS überführt. Zur Wahrung aller bestehenden SEO-Rankings hat der Auftragnehmer zudem ein lückenloses 301-Umleitungskonzept (URL-Redirect-Mapping) zu erstellen und automatisiert auf Infrastrukturebene einzurichten.

3.5 Kooperation mit dem Bestandsdienstleister

Die Migration erfolgt in einer Übergangsphase, in der der bisherige Betriebs- und Entwicklungsdienstleister der KKH weiterhin beauftragt ist und unterstützend mitwirkt.

- **Federführung & Schnittstellendefinition:** Der neu zu beauftragende Auftragnehmer übernimmt die technische Federführung der Migration. Er definiert frühzeitig im Feinkonzept die konkreten Anforderungen an den Datenexport (Schnittstellen, Datenstrukturen, Formate, Zeichensätze, Medienpakete) und stimmt diese mit dem Bestandsdienstleister ab. Der Bestandsdienstleister stellt darauf basierend die Schnittstellen bzw. Daten-Exporte bereit.
- **Kollaborativer Ablauf:** Der Auftragnehmer stimmt Test-Migrationen, Downtimes sowie das finale Cutover-Szenario in enger fachlicher und technischer Abstimmung mit den Bestandsdienstleistern und dem Projektteam der KKH ab.
- **Abgrenzung der Mitwirkungspflichten:** Die Aufgaben der KKH beschränken sich im Wesentlichen auf die Freigabe der Migrationsregeln sowie die stichprobenartige Qualitätssicherung nach dem automatisierten Import. Der Auftragnehmer weist im Bieterangebot aus, welche konkreten Zuarbeiten und Mitwirkungspflichten er vom Bestandsdienstleister und der KKH erwartet.

3.6 Befähigung & Systemeinführung

Nach erfolgreicher automatisierter Befüllung des Systems führt der Auftragnehmer zielgruppengerechte Schulungen für das KKH-Redaktions- und Administrator-Team durch. Da das System zu diesem Zeitpunkt bereits mit den echten, migrierten Inhalten befüllt ist, erfolgt die Einweisung direkt an praxisnahen Anwendungsfällen der KKH.

3.7 Vertragslaufzeit und Vergütung

Der Vertrag hat eine Mindestvertragslaufzeit von 2 Jahren ab Zuschlagserteilung. Der Vertrag verlängert sich automatisch um jeweils ein weiteres Vertragsjahr, sofern dieser nicht von einer der Vertragsparteien mit einer Frist von 12 Monaten zum Ende der jeweiligen Vertragslaufzeit gekündigt wird.

Die Hauptleistungspflichten des Vertrags bestehen in der fortlaufenden Bereitstellung der Plattform sowie deren laufendem Betrieb und Wartung.

Die optionalen Leistungen, insbesondere die kontinuierliche Weiterentwicklung der Plattform, zusätzliche Schulungen und die Bereitstellung von Online-Rechnern, werden bei Bedarf auf Abruf in Form von Einzelaufträgen beauftragt. Eine Verpflichtung zur Abnahme dieser optionalen Leistungen besteht nicht.

Bei Rechnungsstellung sind Fremdkosten auszuweisen und die entsprechenden Belege mit einzureichen. Dies betrifft Leistungen von Drittanbietern (z.B. Suchserver, Monitoring-Tools), die zusätzlich benötigt werden und nicht selbständig von dem Auftragnehmer ausgeführt werden können.

3.8 Ablaufplan

Im Rahmen der Angebotsphase ist von dem Bieter gemäß Kriterienkatalog ein Ablaufplan übersichtlich darzustellen, in welchen Arbeitspaketen und Meilensteinen die Umsetzung im vorgegebenen Zeitfenster zu erfolgen hat.

4. Anforderungen

Dieser Abschnitt beschreibt die fachlichen, technischen, organisatorischen und produktspezifischen Anforderungen an den Auftragnehmer sowie an das zu beschaffende System.

4.1 Anforderungen an den Auftragnehmer

4.1.1 Leistungsfähigkeit und Kompetenzprofil

Der beauftragte Auftragnehmer muss in der Lage sein, sämtliche Leistungsbereiche des Projekts zu erbringen. Dies umfasst Konzeption, UX/UI-Design, Frontend- und Backend-Entwicklung, CMS-Implementierung, Schnittstellenentwicklung, Migration, DevOps, Qualitätssicherung, Betrieb sowie angrenzende Kompetenzen in den Bereichen Barrierefreiheit, Datenschutz und IT-Sicherheit.

Erfahrung in der Realisierung komplexer Webplattformen für regulierte Branchen (Gesundheitswesen, Versicherungen, öffentliche Auftraggeber) ist nachzuweisen. Die Plattform muss die besonderen Anforderungen an Datenschutz (insbesondere Sozialdatenschutz), IT-Sicherheit (BSI-Standards) und Barrierefreiheit (BITV 2.0) erfüllen.

Der Auftragnehmer tritt gegenüber der KKH als verantwortlicher Dienstleister und zentraler Ansprechpartner für den gesamten Leistungsumfang auf, auch soweit einzelne Teilleistungen durch Unterauftragnehmer erbracht werden.

Der Auftragnehmer hat einen für die KKH verantwortlichen, deutschsprachigen Projektleiter zu benennen. Die Gesamtprojektleitung obliegt der KKH.

4.1.2 Personalausstattung: Qualifikationsprofile

Für die Relaunch-Phase sowie den laufenden Betrieb ist ein interdisziplinäres Projektteam bereitzustellen, das alle für die Leistungserbringung erforderlichen Kompetenzen, u. a. Projektleitung, technische Architektur, Frontend- und Backend-/CMS-Entwicklung, UX/UI, Qualitätssicherung, DevOps sowie begleitend Barrierefreiheit und SEO/GEO, abdeckt.

Für den laufenden Betrieb nach dem Relaunch ist ein reduziertes Team vorzusehen. Die konkrete Rollenverteilung, Teamgröße und Kapazitätsplanung ist dem Auftraggeber nach Zuschlagserteilung mitzuteilen.

Zur vertragsgemäßen Erfüllung des Leistungsgegenstandes muss der Auftragnehmer die bedarfsgerechte Bereitstellung von IT- und Digital-Fachkräften mit den entsprechenden Qualifikationsprofilen gewährleisten. Um das geforderte Leistungsspektrum vollumfänglich abzudecken, sind spezifische Rollen erforderlich. Einzelne Personen können bei nachgewiesener Eignung auch mehrere Profile (max. begrenzt auf 2 Profile) abdecken.

Ein Mitarbeiter gilt als ausreichend qualifiziert, wenn er die geforderten Ausprägungen der Qualifikationsstufen (0–4) erfüllt sowie folgende Grundvoraussetzungen nachweist:

- **Ausbildung/Studium:** Erfolgreich abgeschlossenes Studium (z. B. Informatik, Medieninformatik, UX-Design) oder eine vergleichbare Berufsausbildung (z. B. Fachinformatiker) oder den Nachweis einer mehrjährigen, gleichwertigen praktischen Berufserfahrung.
- **Berufserfahrung:** Das eingesetzte Personal für die Position muss entweder folgende Voraussetzung erfüllen:
 - Erster Ansprechpartner/Senior-Rollen: Mindestens 5 Jahre einschlägige Berufserfahrung im entsprechenden Fachgebiet

ODER

 - Experten-/Fachrollen: Mindestens 3 Jahre einschlägige Berufserfahrung.
- **Referenzen:** Aktive Mitarbeit an mindestens zwei vergleichbaren Relaunch- oder Webprojekten (vorzugsweise im regulierten Umfeld oder öffentlichen Sektor) innerhalb der letzten 3 Jahre.
- **Vertretungsregelung:** Für alle Fachexperten muss im Bedarfsfall ein namentlich benannter Vertreter mit vergleichbarem Profil zur Verfügung stehen.
- **Soft Skills:** Team- und Kommunikationsfähigkeit, eigenverantwortliche Arbeitsweise sowie ein hohes Maß an Belastbarkeit und Flexibilität werden vorausgesetzt.

Bewertungssystem der Qualifikationsstufen (Skill-Matrix)

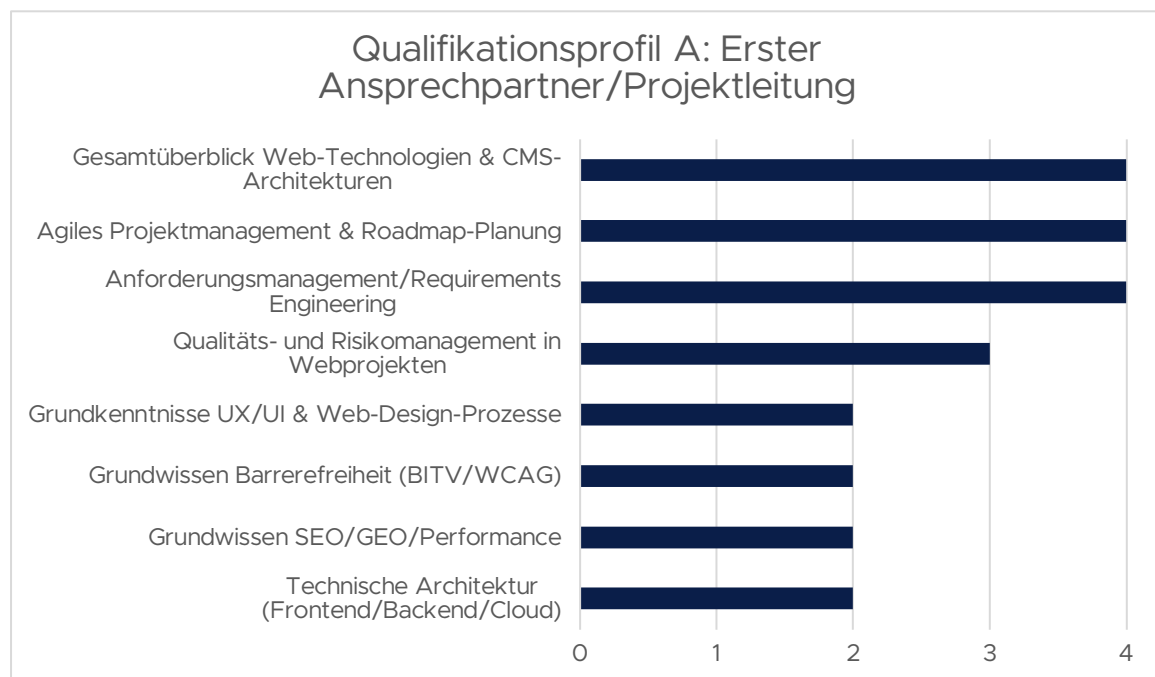
Die detaillierten Qualifikationsanforderungen der jeweiligen Profile werden anhand eines 5-stufigen Raster-Modells (0 bis 4) bewertet:

Profil-Stufe	Beschreibung der Qualifikationsprofil-Ausprägung
0 - keine	
1 - einordnen	MitarbeiterIn hat Überblickswissen, kann das Thema einordnen.
2 - kennen	MitarbeiterIn hat Überblickswissen, kann das Thema einordnen und unter Anleitung in dem Fachgebiet arbeiten. Ist für das Thema/Modul zertifiziert oder hat vergleichbare/nachweisbare Erfahrungen in mindestens einem Projekt gesammelt.
3 - können	MitarbeiterIn hat praktische Erfahrungen mit dem Thema und kann in dem entsprechenden Fachgebiet selbstständig arbeiten. Ist für das Thema/Modul zertifiziert oder hat vergleichbare/nachweisbare Erfahrungen in mindestens einem Projekt gesammelt.
4 - beherrschen	MitarbeiterIn kann selbstständig und routiniert in dem Thema arbeiten. Selbständige Erstellung von Ergebnistypen. Ist für das Thema/Modul zertifiziert oder hat vergleichbare/nachweisbare Erfahrungen in mindestens drei Projekten gesammelt. Koordination und fachliche Verantwortung von Arbeitspaketen und Vermitteln von Wissen in seinem/ihrem Fachgebiet an ProjektmitarbeiterInnen.

Spezifische Qualifikationsprofile

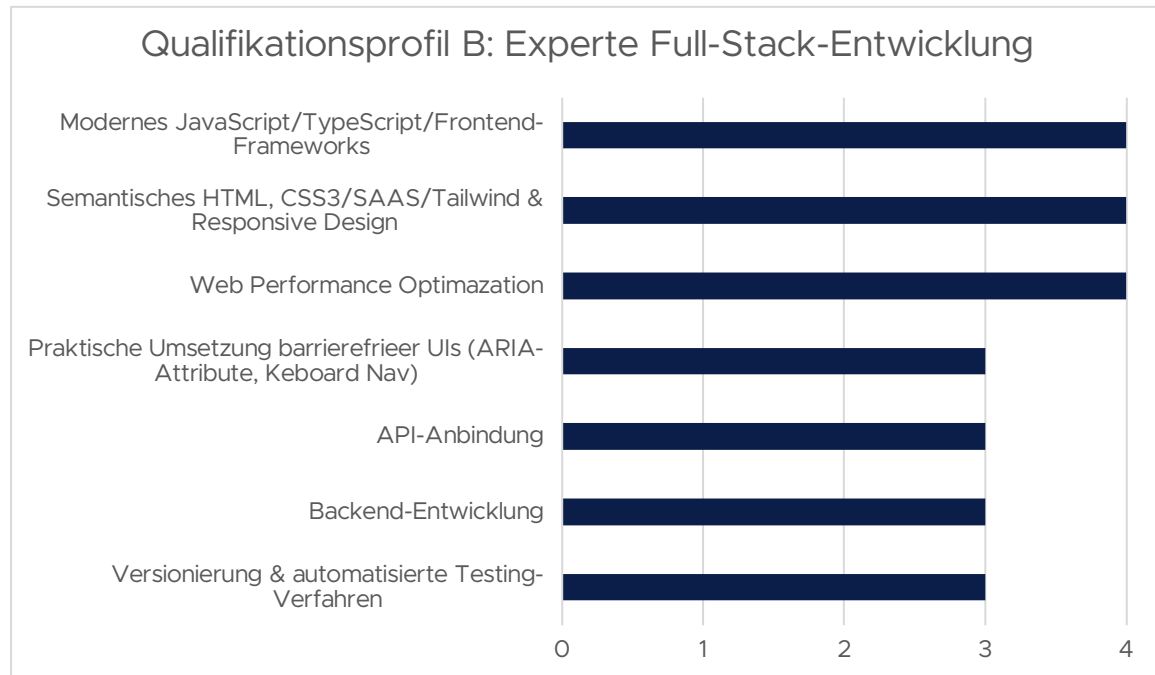
Qualifikationsprofil A: Erster Ansprechpartner/Projektleitung

Die zentrale Funktion des Ersten Ansprechpartners ist die durchgehende, namentliche Steuerung über die gesamte Vertragslaufzeit. Er/Sie nimmt Anforderungen auf, skizziert Lösungsszenarien, steuert das Auftragnehmer-Team und zieht bei Bedarf Fachexperten hinzu.



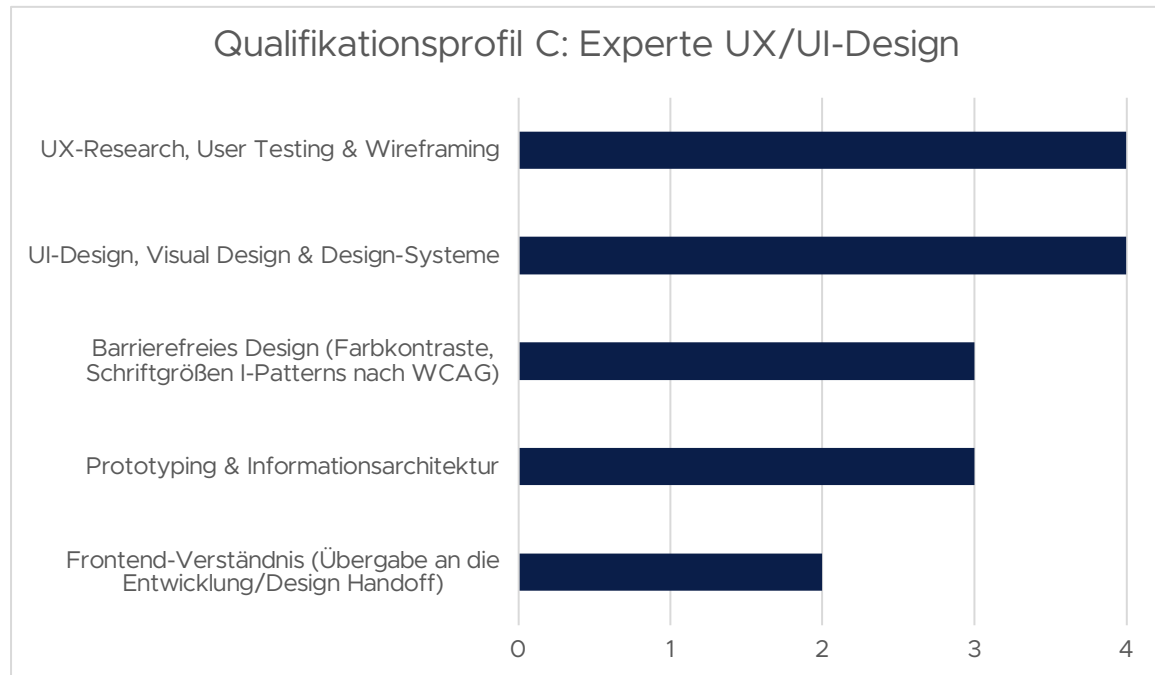
Qualifikationsprofil B: Experte Full-Stack-Entwicklung

Der Experte ist verantwortlich für die technische Umsetzung der Benutzeroberflächen, Komponentenbibliotheken und der Anbindung an Backend-Systeme/APIs.



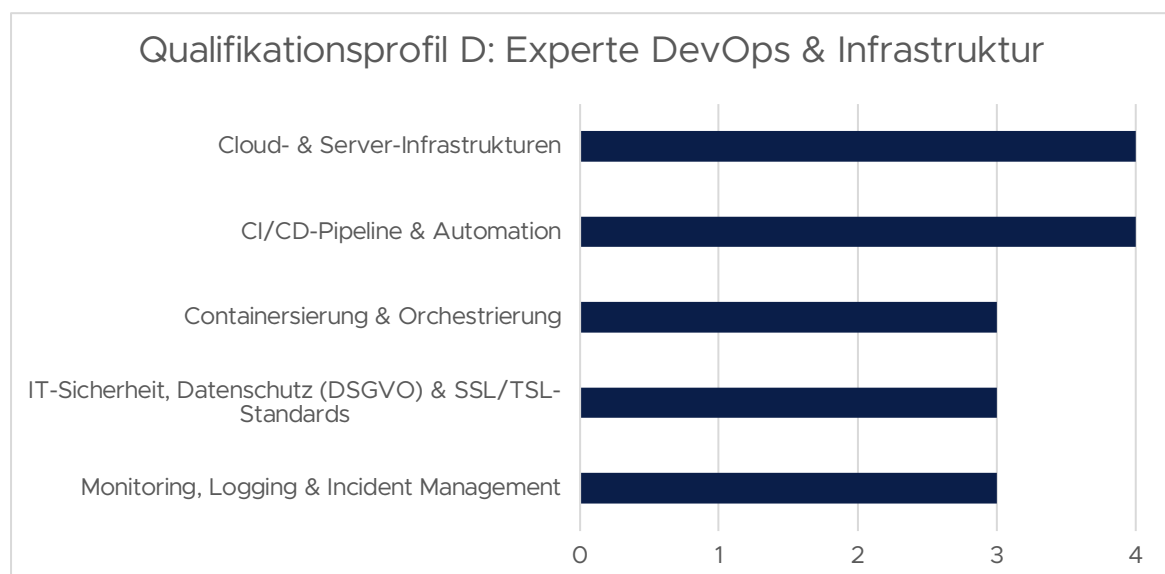
Qualifikationsprofil C: Experte UX/UI-Design

Verantwortlich für die Konzeption, Gestaltung und Nutzbarkeit der digitalen Schnittstellen unter Berücksichtigung von Design-Systemen und Barrierefreiheit.



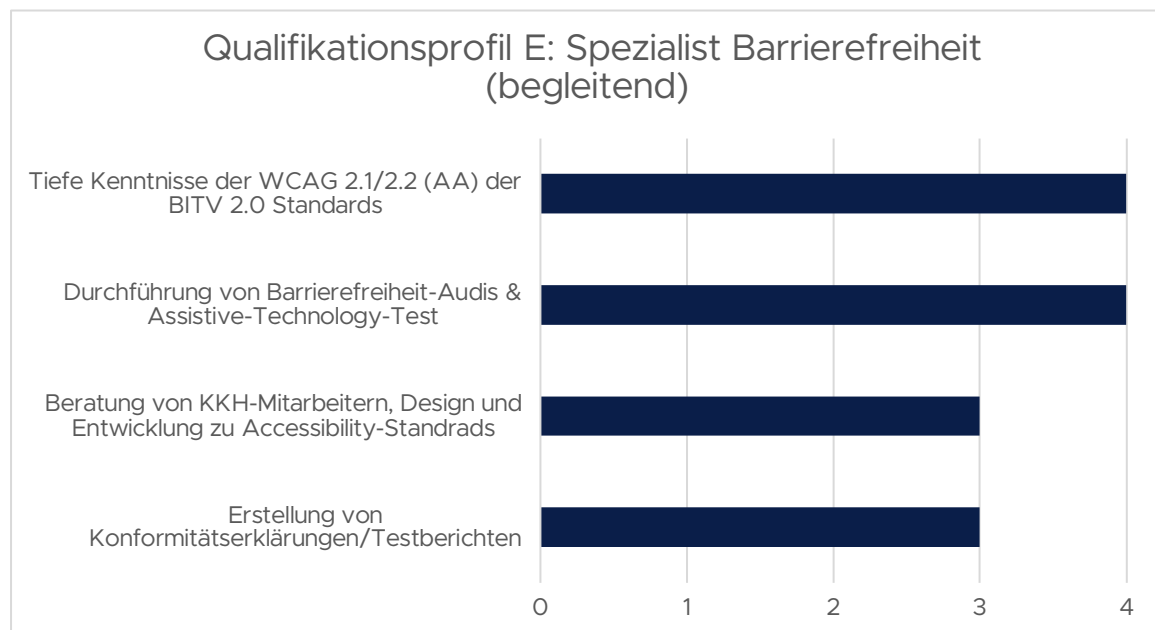
Qualifikationsprofil D: Experte DevOps & Infrastruktur

Sichert den reibungslosen Betrieb, die Deployment-Pipelines, Hosting-Infrastrukturen sowie die Einhaltung von IT-Sicherheitsstandards.



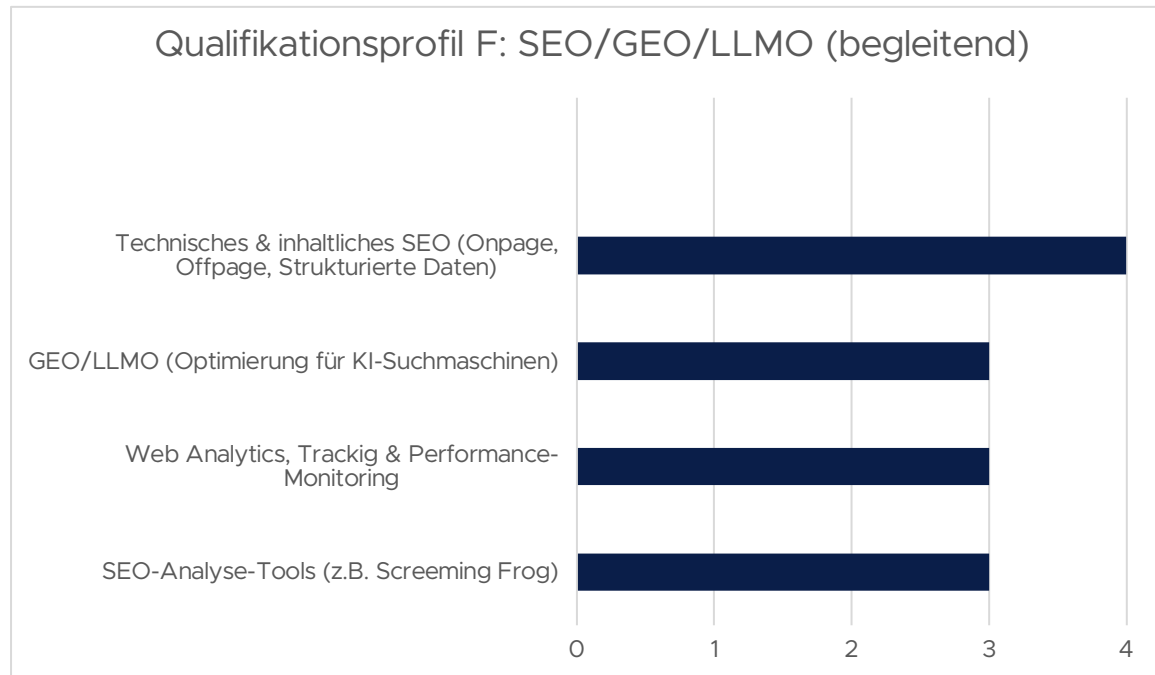
Qualifikationsprofil E: Spezialist Barrierefreiheit (begleitend)

Stellt sicher, dass das Webangebot den gesetzlichen Vorgaben zur Barrierefreiheit (BITV 2.0 / WCAG 2.1/2.2 AA / EAA) vollumfänglich entspricht.



Qualifikationsprofil F: Spezialist SEO/GEO/LLMO (begleitend)

Optimiert das Webangebot sowohl für klassische Suchmaschinen (SEO) als auch für KI-gestützte Generative Search Engines (GEO) und Large Language Model Discovery (LLMO).



Darüber hinaus sind die Profile der Anlage „Allgemeinen Rahmenbedingungen IT-Servicemanagement“ (vgl. Kapitel 2.1) ebenfalls einzureichen.

4.1.3 Wissenstransfer und Projektsicherheit

Der Auftragnehmer hat sicherzustellen, dass Projektwissen nicht an einzelnen Personen hängt. Hierfür sind folgende Maßnahmen verbindlich umzusetzen:

- Kontinuierliche Dokumentation aller Projektergebnisse, Architekturentscheidungen und Prozesse in einem zentralen Projektwiki (z.B. Confluence)
- Regelmäßige Code-Reviews und Pair-Programming zur Verteilung des technischen Wissens
- Doppelbesetzung kritischer Rollen
- Strukturierter, dokumentierter Übergabeprozess bei Personalwechsel
- Langfristige Teamstabilität für Kernrollen über die gesamte Vertragslaufzeit

4.1.4 Referenzen und Branchenerfahrung

Der Auftragnehmer ist verpflichtet, vergleichbare Projekte gemäß Anlage Eignungsnachweise nachzuweisen.

4.1.5 Interessenkonflikte

Es muss immer gewährleistet sein, dass ein eigenständiges Team den Auftraggeber betreut. Während der Dauer der Zusammenarbeit mit dem Auftraggeber dürfen die vom Auftragnehmer für die Leistungserbringung beim Auftraggeber eingesetzten Mitarbeiter für keinen Auftraggeber aus dem Bereich der deutschen gesetzlichen Krankenversicherung tätig werden. Bei Zweifeln hat sich der Auftragnehmer mit dem Auftraggeber abzustimmen und dessen Entscheidung Folge zu leisten. Etwaige Interessenkonflikte sind durch organisatorische Maßnahmen auszuschließen (strikte Mandantentrennung, separate Projektteams, Chinese Walls etc.).

Diese Regelung gilt für das betreuende Kern-Team während der gesamten Vertragslaufzeit. Das heißt, dass sämtliche Mitarbeitende, die in die strategische sowie operative Leistungserbringung für den Auftraggeber involviert sind, parallel nicht für weitere Kunden aus dem Bereich der gesetzlichen Krankenkassen tätig sein dürfen. Hiervon ausgenommen sind Personen, die mit nachgelagerten Prozessen wie der Rechnungsstellung betraut sind.

4.1.6 Versicherungssummen

Der Auftragnehmer hat folgende Mindestversicherungssummen gemäß Anlage Eignungsnachweise nachzuweisen:

- Betriebshaftpflicht Personen-/Sachschäden: mind. 1.000.000 € je Versicherungsfall
- Vermögensschäden (inkl. Datenschutz/Cyber): mind. 5.000.000 € je Versicherungsfall

4.2 Anforderungen an Vorgehensmodell und Projektorganisation

4.2.1 Vorgehensmodell

Das Projekt ist nach einem agilen Vorgehensmodell durchzuführen. Agil bedeutet in diesem Kontext: iterative, inkrementelle Leistungserbringung in kurzen, review-basierten Zyklen mit kontinuierlicher Priorisierung des Backlogs und enger, fortlaufender Abstimmung mit dem Auftraggeber, im Gegensatz zu einer starren Wasserfallplanung mit einmaliger Anforderungsdefinition zu Projektbeginn.

Für die Relaunch-Phase ist Scrum verbindlich einzusetzen, ergänzt um Kanban-Elemente im laufenden Betrieb. Abweichende oder hybride Modelle sind zu begründen und mit der KKH abzustimmen.

Konkrete Anforderungen an das Vorgehen sind:

- Sprints von 2 bis 3 Wochen Länge mit definierten Sprint-Zielen
- Daily Stand-ups (max. 15 Minuten), Sprint Planning, Sprint Review und Retrospektive
- Priorisierter Backlog, der kontinuierlich gemeinsam mit dem Auftraggeber gepflegt wird
- Transparente Fortschrittssteuerung über Burndown-Charts und Kanban-Boards
- Im laufenden Betrieb: Kanban-Betrieb mit priorisiertem Backlog

4.2.2 Anforderungsmanagement

Anforderungen sind strukturiert als Epics, User Stories und Akzeptanzkriterien zu dokumentieren. Priorisierung erfolgt gemeinsam mit dem Auftraggeber nach fachlichem Mehrwert, Risiko, Aufwand und regulatorischer Relevanz.

4.2.3 Beauftragung von Einzelaufträgen

Die Erbringung projektspezifischer Leistungen sowie von Weiterentwicklung und Anpassungsbedarfen im Nachgang zum Relaunch (Betriebs- und Weiterentwicklungsphase) erfolgt stufenweise über den Abruf von Einzelaufträgen. Entsteht beim Auftraggeber ein konkreter Leistungsbedarf, übermittelt er dem Auftragnehmer eine entsprechende Aufgabenbeschreibung. Der Auftragnehmer erstellt daraufhin ein verbindliches Angebot mit einer detaillierten Aufwandsschätzung. Dieses Angebot muss einen Kostenvoranschlag gemäß Preisblatt sowie einen Zeitplan unter Berücksichtigung der in der Leistungsbeschreibung genannten Verpflichtungen und Anforderungen enthalten.

Nach erfolgreicher fachlicher und kaufmännischer Prüfung durch den Auftraggeber erteilt dieser den schriftlichen Einzelauftrag und übermittelt den Auftragnehmer eine entsprechende kaufmännische Bestellung. Erst mit dem Zugang dieser offiziellen Bestellung gilt die Ausführungsfreigabe als erteilt, und der Auftragnehmer ist berechtigt sowie verpflichtet, mit der Umsetzung der definierten Leistungen zu beginnen. Vor dem offiziellen Bestelleingang eigeninitiativ erbrachte Aufwände oder Vorarbeiten des Auftragnehmers gelten als nicht beauftragt und werden vom Auftraggeber nicht vergütet.

4.2.4 Toolset und Kommunikation

Der Auftragnehmer hat im Rahmen der Angebotsphase ein praxiserprobtes und integriertes Toolset für die Zusammenarbeit und Projektsteuerung vorzuschlagen. Das vorgeschlagene Toolset muss mindestens folgende Funktionsbereiche abdecken:

- Projektsteuerung & Ticketing (z.B. Jira)
- Dokumentation & Wissensmanagement (z.B. Confluence)
- Design & Prototyping (z.B. Figma)

- Code-Verwaltung & CI/CD (z.B. GitLab oder GitHub)
- Kommunikation: Microsoft Teams als verbindlicher Kommunikationskanal für die projektbezogene Zusammenarbeit und Regelkommunikation

Die Nutzung von Microsoft Teams erfolgt bevorzugt innerhalb der von der KKH bereitgestellten bzw. freigegebenen Microsoft-365-/Teams-Umgebung, um eine einheitliche, administrierbare und datenschutzkonforme Kommunikation sicherzustellen.

Der Auftragnehmer hat im Angebot darzulegen, welche konkreten Werkzeuge eingesetzt werden sollen und wie der Zugriff sowie der sichere Datenaustausch für die KKH gewährleistet werden.

Die im Rahmen des Projekts erstellte Dokumentation und das vollständige Wissensmanagement stehen der KKH jederzeit vollständig zur Verfügung. Sämtliche Inhalte sind spätestens bei Übergabe bzw. Vertragsende in einem mit der KKH abgestimmten, offenen und weiterverarbeitbaren Format bereitzustellen. Proprietäre Formate oder technische Abhängigkeiten, die eine weitere Nutzung, Migration oder Übernahme durch die KKH bzw. einen Nachfolgendienstleister einschränken, sind zu vermeiden.

Code-Verwaltung und CI/CD erfolgen ausschließlich in einer geschützten, nicht öffentlich zugänglichen Umgebung. Repositories sind als private Repositories zu betreiben und durch rollenbasierte Berechtigungen, MFA, Protokollierung, sichere Secret-Verwaltung sowie angemessene Zugriffsbeschränkungen abzusichern. Eine Ablage von KKH-Quellcode, Konfigurationen, Zugangsdaten oder sonstigen schützenswerten Informationen in öffentlichen Repositories ist auszuschließen.

Sämtliche Kosten für das vorgeschlagenen Toolset (inkl. 2 Nutzungs- bzw. Betrachter-Lizenzen für KKH-Produktmanagement und Stellvertretung) sowie alle Aufwände für die Vorbereitung, Durchführung und Nachbereitung der regulären Abstimmungs- und Steuerungsformate sind vollumfänglich in die laufenden Betriebsaufwände einzupreisen.

Der KKH ist während der Projektlaufzeit aktiver Zugriff (mind. 2 Named User) auf die zentralen Tools zu gewähren, inkl. Anlage und Bearbeitung von Tickets im Projektmanagement-Tool.

Die regelmäßige Abstimmung ist über verbindliche Formate sicherzustellen. Hierzu zählen mindestens wöchentliche Status-Calls, monatliche Steuerungsrounds sowie quartalsweise Strategie- und Roadmap-Reviews zur Überprüfung der übergeordneten Meilensteine.

Darüber hinaus sind die Service Meetings laut Anlage Allgemeine Rahmenbedingungen IT-Servicemanagement (vgl. Kapitel 2.4) einzuhalten und einzukalkulieren.

4.2.5 Projektstart und Zusammenarbeit

Die initiale Projektphase dient der gemeinsamen Zielschärfung und der Herstellung eines belastbaren Projektfundaments. Sie umfasst:

- Kick-off-Workshop (1 bis 2 Tage): Kennenlernen aller Beteiligten, Klärung von Rollen, Kommunikationswegen, Tools und übergeordneten Projektzielen

- Fachliche und technische Workshops zur Anforderungserhebung (Schnittstellen, Inhaltsstruktur, Zielarchitektur, Redaktionsprozesse)
- Technische Analysephase: Auditierung der bestehenden AEM-Infrastruktur, Schnittstellen und Inhalte
- Gemeinsame Backlog-Erstellung und Roadmap-Definition

4.3 Anforderungen an das CMS

4.3.1 Systemauswahl und Empfehlung

Das CMS muss einem modularen und erweiterbaren Systemaufbau unterliegen. Neue Funktionen müssen sich nahtlos integrieren lassen. Zudem wird eine containerbasierte cloud-ready Architektur gefordert, die den flexiblen Betrieb in unterschiedlichen Infrastrukturen erlaubt.

Zudem ist das CMS so zu wählen, dass es den spezifischen Anforderungen einer gesetzlichen Krankenkasse gerecht wird. Maßgebliche Kriterien sind:

- Eignung für regulierte Branchen (Sicherheit, Datenschutz, Compliance)
- Nachgewiesene Skalierbarkeit für umfangreiche Enterprise-Websites
- Umfassendes Rollen- und Rechtemanagement
- Unterstützung von Barrierefreiheit (BITV 2.0/WCAG 2.2 AA)
- EU-Cloud mit vollständiger Datensouveränität (kein US-Hyperscaler)
- Herstellerunabhängigkeit und Wartbarkeit
- Etablierung am Markt seit mindestens 2 Jahren, mit regelmäßigen Updates und Zukunftsfähigkeit durch Hersteller oder Community
- Vollständige Verfügbarkeit der Redaktionsoberfläche in deutscher Sprache
- Abbildbarkeit des Full-Stack-Ansatzes (Konzeption bis Betrieb)

4.3.2 Lizenzmodell und Kosten

Es ist ein Open-Source-System ohne wiederkehrende Lizenzgebühren einzusetzen (z. B. TYPO3, Umbraco, Wagtail). Eigenentwicklungen des CMS-Kernsystems durch den Auftragnehmer sind ausgeschlossen.

Das System muss für den parallelen Zugriff von mind. 15 gleichzeitig aktiven Redakteuren (Concurrent User/Floating Lizenzmodell) ausgelegt sein. Das CMS darf technisch keine Limitierung hinsichtlich der Gesamtzahl anzulegender, personengebundener Benutzerkonten (Named User) aufweisen und darf hierfür keine lizenzkostenpflichtigen Beschränkungen vorsehen. Die initiale Einrichtung der Admin- und Redaktionszugänge erfolgt nach Absprache im Rahmen des Projekts.

Updates sind im Pauschalpreis zur Bereitstellung und Pflege des CMS einzukalkulieren.

4.3.3 Rollen- und Rechtemanagement

Das CMS muss ein granulares, rollenbasiertes Rechtemanagement unterstützen. Folgende Mindestanforderungen sind:

- Beliebig viele Benutzergruppen mit individuellen Rechten (z. B. Zentralredakteur, Regionalredakteur, Fachbereichsprüfer, Administrator)
- Berechtigungen auf Seiten-, Inhaltstyp- und Feldebene
- Mehrstufige Redaktionsworkflows mit Freigabeprozessen (Vier-Augen-Prinzip)
- Personenbezogene Logins, keine gemeinsamen Accounts; Zugriffsprotokolle
- Benutzerverwaltung: Anlegen, Pflegen und Löschen von Benutzern, Rollen und Gruppen; mehrere Rollen pro Benutzer müssen möglich sein
- Frei definierbare Rollen, mindestens Administrator, Redakteur und Autor
- Multi-Faktor-Authentifizierung (MFA) für administrative und privilegierte Konten
- Umsetzung des Least-Privilege-Prinzips
- Regelmäßige Berechtigungsrezertifizierung
- Möglichst Just-in-Time-Zugriffe (JIT) und Privileged Access Management (PAM)

4.3.4 Content-Pflege und Redaktionsfunktionen

Die Redaktionsumgebung ist so zu gestalten, dass Inhalte effizient, intuitiv und ohne technische Vorkenntnisse gepflegt werden können. Folgende Mindestanforderungen sind:

- In-Site-Editing: direkte Bearbeitung von Inhalten auf der Website nach Login
- Vorschaufunktion vor der Veröffentlichung, für Desktop- und mobile Ansicht
- Zeitgesteuertes Aktivieren/Deaktivieren von Seiten sowie Passwortschutz einzelner Seiten
- Versionierung und Undo-Funktion, sowohl für einzelne Objekte als auch für komplette Website-Versionen
- Wiedervorlage-Prozess: Einstellbare Prüffristen pro Seite mit systemseitiger Auswertung, automatischen Reminder-E-Mails an Verantwortliche sowie einer zentralen Übersicht im Backend; Live-Seiten bleiben während der Prüfung unterbrechungsfrei aktiv
- Textbearbeitung über WYSIWYG-Editor mit Übernahme von Formatierungen, integrierter Rechtschreibprüfung, Multilingualität und Quelltextkomponenten

- Social-Media-Integration sowie ein automatisch oder individuell gestaltbarer RSS-Feed

Weitere zusätzliche Funktionalitäten sind nicht zwingend erforderlich, diese werden jedoch im Kriterienkatalog positiv bewertet:

- KI-gestützte Textvorschläge im Redaktionsmodus
- Sicherheitsabfragen für kritische Aktionen
- Vorschau-Links für Freigaben durch Fachbereiche inklusive Kommentarfunktion
- Übersetzungsfunktionen für ausgewählte Seiten
- Seitensuche im Redaktionsmodus, die auch URLs auffindet
- Mechanismen zur Unterstützung wiederkehrender und kleinteiliger Redaktionsaufgaben

4.3.5 Komponenten, Templates und Containerlösung

Für die flexible Gestaltung von Inhalten sind folgende Anforderungen an Templates und Komponenten verbindlich:

- Flexible Containerlösung: Inhalte und Komponenten sind frei positionierbar, können kopiert und zwischen Seiten wiederverwendet werden
- Drag-and-Drop-Funktionalität für Seitenbaum und Navigation; Baumstruktur für Navigation und Seitenorganisation
- Templates mit maximalem gestalterischem Spielraum, ohne Vererbung von übergeordneten Seiten auf Unterseiten
- Vollständig responsive Komponenten (Mobile First/Fluid Layout): Automatische und fehlerfreie Anpassung aller Layouts und Medien an sämtliche Screen-Größen und Viewports (Desktop, Tablet, Mobile) inkl. Touch-optimierter Bedienelemente (z.B. ausreichend große Klickflächen nach WCAG) sowie einer integrierten Breakpoint-Vorschau im Redaktionssystem
- Vorhandene Basiskomponenten, z. B. Bilder- und Videogalerie
- Verfügbarkeit aller Komponenten für alle Seiten und Templates
- Individuelle Konfigurierbarkeit einzelner Komponenten (z. B. Farbeinstellungen)
- Eindeutiger Bearbeitungsmodus, klar erkennbar, an welcher Stelle einer Komponente Inhalte bearbeitet werden können
- Möglichkeit zur Entwicklung individueller neuer Komponenten

4.3.6 Medien- und Asset-Management

Für die Verwaltung von Medien und Assets gelten folgende Mindestanforderungen:

- Zentrale Verwaltung von Grafiken, Audio-, Video- und Dokumentendateien
- Filter- und Versionsfunktionen
- Zoom-in-Funktion, Skalierung, Zuschchnitt, Mehrfachverwendung und Versionierung von Grafiken
- Performance-Optimierung inkl. automatischer Asset-Komprimierung (WebP und AVIF)
- Flexibler Einsatz von Videos, z. B. im Header-Slider

Weitere zusätzliche Funktionalitäten sind nicht zwingend erforderlich, diese werden jedoch im Kriterienkatalog positiv bewertet:

- Automatische farbliche Anpassung von SVG-Dateien

4.3.7 Mehrsprachigkeit

Mehrsprachigkeit ist als native CMS-Funktion sicherzustellen. Das System muss beliebig viele Sprachvarianten unterstützen. Für die KKH ist mindestens Deutsch als Hauptsprache und Englisch als Zweitsprache mit der Option zur Erweiterung um weitere Sprachen (inkl. Leichte Sprache, Gebärdensprache gemäß BITV 2.0) vorzusehen. Sprachfallbacks, hreflang-Tags und XLIFF-Export für externe Übersetzungsdienstleister sind erforderlich.

Weitere zusätzliche Funktionalitäten sind nicht zwingend erforderlich, diese werden jedoch im Kriterienkatalog positiv bewertet:

- Übersetzung aller Elemente der Seiten (z. B. auch Header und Footer)
- Automatisierte Übersetzung aller deutschen Inhalte
- Indexierung zur Auffindbarkeit bei Google
- Seiten sollen trotz automatisierter Übersetzung individuell bearbeitbar sein
- Seiten sollen unabhängig der deutschen Version ergänzt oder offline gestellt werden können
- Einbindung von Tools unabhängig der deutschen Seite (z. B. Seminarbuchung)
- Tools der deutschen Version müssen eliminierbar sein (z. B. Terminservice SST)

4.3.8 Inhaltsmodelle und Flexibilität

Inhaltsmodelle sind so zu konzipieren, dass sie ohne Systembruch erweitert werden können. Anforderungen:

- Komponentenbasierter Aufbau (Baukastenprinzip) für redaktionelle Flexibilität
- Versionierte Datenbankmigrationen bei Modellerweiterungen
- Headless-Option für kanalunabhängige Inhaltsauspielung

- Anbindung externer Systeme über APIs ohne Einschränkungen durch das Inhaltsmodell

4.3.9 Suchfunktion

Das CMS muss eine integrierte Suchfunktion bereitstellen. Die Mindestanforderungen lauten wie folgt:

- Volltextsuche über Inhalte und Metadaten, mit Autovervollständigung und Korrekturvorschlägen
- Nutzerfreundliche Bedienung mit hoher Trefferquote, insbesondere für die Seitensuche und die Servicestellensuche
- Statistik zu Suchanfragen, häufigen Suchbegriffen und Trefferquote

4.3.10 Schnittstellenintegration

Der Auftragnehmer ist für die Konzeption, Anbindung, Migration und den dauerhaft stabilen Betrieb aller externen Schnittstellen und Drittsysteme verantwortlich. Zu den im Rahmen des Projekts zu integrierenden Anbindungen und Systemen gehören insbesondere:

- Newsletter-Systeme (aktuell AIC Group)
- Bewerbermanagement-Tools (aktuell Concludis)
- Karten- und Standortdienste (aktuell 123map)
- Suchsysteme (derzeitig Eigenentwicklung des aktuellen Auftragnehmers, Übernahme oder Migration auf ein modernes Suchsystem)
- Online-Terminbuchung: Der Auftragnehmer hat einen datenschutz- und cloud-compliance-konformen Dienstleister vorzusehen, der die erforderlichen Datenschutz- und Sicherheitsnachweise (insbesondere ein gültiges C5-Testat) erbringt.
- Web-Controlling: DSGVO-konforme Erfassung von Zugriffszahlen und Nutzungsdaten inkl. Filterung, Export und Einbindung externer Tools (aktuell eTracker)
- CRM- und Backend-Systeme
- Social-Media- und Video-Einbindungen (datenschutz- und DSGVO-konform)
- Einbindung externer Widgets und iFrames, z. B. Online-Rechner (vgl. Abschnitt 4.3.11)

Sämtliche Schnittstellen sind mit einem definierten Fehler-Handling (Error-Handling), automatisierten Retry-Mechanismen, konfigurierbaren Timeouts, strukturiertem Logging sowie einem automatisierten Alerting (z. B. Benachrichtigung bei Systemausfällen) und kontinuierlichen Health-Checks aufzubauen und zu betreiben. Bestehende und funktionierende Schnittstellen sind ohne Unterbrechung des Live-Betriebs funktionsfähig in das neue System zu übernehmen.

4.3.11 Online-Rechner

Der Auftragnehmer muss untenstehende Online-Rechner auf der Website zur Verfügung stellen können, welche im Rahmen eines Einzelauftrags zu Vertragsbeginn abgerufen werden.

Übergreifende fachliche Anforderungen (für alle Rechner):

- Gesetzliche & tarifliche Aktualität: Automatische und zeitnahe Anpassung aller Rechenlogiken, Freibeträge, Beitragsbemessungsgrenzen und sonstigen Rechenparameter an gesetzliche oder verordnete Änderungen zum Stichtag des Inkrafttretens
- Barrierefreiheit: Vollständige Erfüllung der Vorgaben nach BITV 2.0 für die Nutzung auf Krankenkassen-Websites (WCAG 2.2 AA)
- Usability & Design: Responsive Darstellung für alle Endgeräte (Desktop, Tablet, Smartphone), intuitive Eingabeführung inkl. verständlicher Hilfetexte/Tooltips zu Fachbegriffen
- Ergebnisdarstellung: Transparente Aufschlüsselung der Rechenwege und verständliche Auskunftstexte für die Versicherten

Spezifische fachliche Mindestanforderungen je Rechner:

a. Fristenrechner

- Exakte Berechnung gesetzlicher und administrativer Fristen unter Berücksichtigung bundeslandspezifischer Feiertage sowie der Sonn- und Feiertagsregelungen
- Eindeutige Ausweisung von Fristbeginn, Fristende und maßgeblichen Ereignisdaten

b. Gehaltsrechner

- Orientierende Erstberechnung auf Basis aktueller Lohnsteuerklassen, Kinderfreibeträge und Beitragsbemessungsgrenzen
- Berücksichtigung der aktuellen Regelungen zum Übergangsbereich (Midijob) und Minijob-Grenzen
- Variable Eingabemöglichkeit des individuellen Zusatzbeitrags der Krankenkasse

c. Mutterschutzrechner

- Berechnung der gesetzlichen Schutzfristen vor und nach der Entbindung auf Basis des voraussichtlichen Entbindungstermins

- Berücksichtigung von Sonderfällen (Frühgeburten, Mehrlingsgeburten, medizinische Behinderung des Kindes) mit automatischer Verlängerung der Schutzfrist nach der Geburt auf 12 Wochen

d. Entgeltfortzahlungsrechner

- Ermittlung des 6-Wochen-Anspruchs (42 Kalendertage) auf Entgeltfortzahlung durch den Arbeitgeber im Krankheitsfall (§ 3 EntgFG)
- Berücksichtigung von Unterbrechungen und Anrechnung von Vorerkrankungszeiten zur Bestimmung des Leistungsbeginns des Krankengeldes

e. KV-Rechner für Selbstständige

- Ermittlung der Beitragsbelastung zur gesetzlichen Kranken- und Pflegeversicherung für freiwillig versicherte Selbstständige
- Erfassung verschiedener Einnahmenarten unter Beachtung der gesetzlichen Mindest- und Höchstbemessungsgrundlagen
- Abbildung der gestaffelten Pflegeversicherungsbeiträge nach Elterneigenschaft und Kinderzahl (PUEG) sowie Wahloptionen für Krankengeldanspruch/Wahltarife

f. Krankengeldrechner

- Berechnung des voraussichtlichen Brutto- und Netto-Krankengeldes gemäß § 47 SGB V (70 % des regelmäßigen Arbeitsentgelts, höchstens 90 % des Nettoarbeitsentgelts unter Beachtung der gesetzlichen Höchstgrenzen)
- Berücksichtigung einmalig gezahlten Arbeitsentgelts der letzten 12 Monate.
- Korrekter Abzug der gesetzlichen Arbeitnehmeranteile zur Sozialversicherung (Renten-, Arbeitslosen- und Pflegeversicherung)

g. Zuzahlungsrechner

- Ermittlung der individuellen Belastungsgrenze nach § 62 SGB V (2 % der jährlichen Bruttoeinnahmen zum Lebensunterhalt bzw. 1 % für chronisch Kranke)
- Berücksichtigung der aktuellen Freibeträge für Ehe-/Lebenspartner und Kinder
- Gegenüberstellung bereits geleisteter Zuzahlungen zur Feststellung einer Befreiung oder Erstattung

h. Brutto-Netto-Rechner

- Zwingende Verwendung des jeweils aktuellsten offiziellen Programmablaufplans (PAP) des Bundesfinanzministeriums (BMF) zur exakten Ermittlung von Lohnsteuer, Solidaritätszuschlag und Kirchensteuer

- Vollständige Abbildung aller Steuerklassen (1–6), des Faktorverfahrens bei Steuerklasse 4, Kinderfreibeträge, Freibeträge auf der Lohnsteuerkarte und Bundesland-Spezifika (Kirchensteuer)
- Exakte Berechnung aller Sozialversicherungsbeiträge (KV, RV, AV, PV) inklusive aller PUEG-Beitragsstaffelungen für Kinder sowie Berücksichtigung von Beitragszuschlägen für Kinderlose
- Berücksichtigung von geldwerten Vorteilen (z. B. Dienstwagenregelung), Altersentlastungsbetrag und Versorgungsfreibetrag

Diese Rechner basieren technisch teilweise auf dem Nachladen von JavaScript aus externen Quellen (aktuelle Anbieter: Smart Rechner und inside partner). Da dies aus IT-Security-Sicht (u. a. Schadcode- und Supply-Chain-Risiko, unkontrollierte Systemänderungen, eingeschränkte Nachvollziehbarkeit, mögliche Gefährdung von Verfügbarkeit sowie Abfluss sensibler Informationen) kritisch zu bewerten ist, gelten für die Einbindung folgende verbindliche Mindestanforderungen, orientiert an den Vorgaben des BSI IT-Grundschutz:

- Ausführung in einer separaten, gekapselten und vom Kernsystem getrennten Umgebung (z. B. isoliertes iFrame/Sandbox)
- Prüfung und Beschränkung der für die Ausführung zwingend erforderlichen Rechte nach dem Least-Privilege-Prinzip
- Aktives Monitoring der zugehörigen Log-Dateien mit automatisierter Alarmierung bei Auffälligkeiten
- Bezug der Skripte ausschließlich aus vertrauenswürdigen, vorab freigegebenen Quellen; Integritätsprüfung (digitale Signaturen bzw. Prüfsummen), sofern verfügbar
- Dokumentiertes, nachvollziehbares Change-, Patch- und Freigabemanagement für alle eingebundenen Drittanbieter-Skripte (wer, wann, was geändert bzw. freigegeben wurde und wie der vorherige Zustand wiederhergestellt werden kann)
- Sicherstellung, dass über die Rechner-Skripte keine sensiblen Informationen (Umgebungsvariablen, Zugangsdaten, Tokens, Kunden- bzw. Versichertendaten) ausgelesen werden können
- Regelmäßige Überprüfung der eingesetzten Skripte auf Herstellersupport, verfügbare Sicherheitsupdates und bekannte Schwachstellen

Der Einsatz ungeprüfter, unbekannter oder nicht freigegebener Skripte in der produktiven Umgebung ist ausgeschlossen. Der Auftragnehmer hat der KKH vor Go-Live ein Konzept zur sicheren Kapselung, Rechtebeschränkung und Überwachung der Online-Rechner vorzulegen und freigeben zu lassen.

4.3.12 Online-Formulare, Online-Beitrittserklärung und E-Mail-Routing

Die CMS-Lösung muss die Erstellung und den sicheren Betrieb einfacher Online-Formulare sowie komplexer, mehrstufiger Antragsstrecken ermöglichen, insbesondere einen möglichst

vollständigen digitalen Online-Beitritt. Die Formulare sind direkt im CMS zu entwickeln, zu integrieren, zu testen und zu betreuen; ein zusätzliches Formular-Management-System ist für die grundlegende Umsetzung nicht zwingend erforderlich. Im Angebot ist darzustellen, welche Funktionen zum CMS-Standard gehören und welche individuell entwickelt werden müssen.

Verarbeitung personenbezogener Daten und Sozialdaten

Im Rahmen der Online-Formulare und insbesondere der Online-Beitrittserklärung werden personenbezogene Daten und Sozialdaten verarbeitet. Für die hierfür eingesetzten Cloud-Dienste und beteiligten Dienstleister sind daher die Anforderungen des § 393 SGB V einschließlich des erforderlichen C5-Nachweises verbindlich anzuwenden. Dies gilt auch für eingebundene Unterauftragnehmer und technische Teildienste, sofern diese Sozialdaten verarbeiten oder Zugriffsmöglichkeiten hierauf besitzen.

Erstellung und Pflege im CMS

Folgende Mindestanforderungen sind:

- Ein- und mehrstufige Formulare direkt im CMS erstellbar
- wiederverwendbare Formularfelder und Komponenten
- bedingte Fragen und dynamische Abläufe abhängig von den bisherigen Angaben
- client- und serverseitige Validierung aller Eingaben; serverseitig gesteuerte Pflichtfelder, Regeln und Plausibilitätsprüfungen
- Pflege von Texten, Hinweisen, Auswahllisten und rechtlichen Erklärungen durch berechtigte KKH-Beschäftigte
- vollständige Übergabe von Quellcode, Konfigurationen, Datenmodellen und Dokumentation an die KKH

Für Rollen- und Rechtekonzept, Versionierung sowie Entwicklungs-, Test-, Abnahme- und Produktivumgebungen gelten die allgemeinen CMS-Anforderungen nach Abschnitt 4.3.3, 4.3.4 und 4.4.2. Die responsive und barrierefreie Umsetzung richtet sich nach Abschnitt 4.6.1 und 4.6.2.

Online-Beitrittserklärung

Der Online-Beitritt muss einen möglichst vollständigen digitalen Antrag ermöglichen. Mindestens vorzusehen sind:

- mehrstufige, nutzerfreundliche Antragsstrecke mit Fragen abhängig von der jeweiligen Lebens- und Versicherungssituation
- Fortschrittsanzeige und verständliche Hinweise zu den nächsten Schritten
- Zwischenspeicherung und spätere Fortsetzung eines Antrags über ein von der KKH freigegebenes, sicheres Verfahren; automatische Löschung nicht abgeschlossener Entwürfe nach festgelegter Frist gemäß Löschkonzept (vgl. Abschnitt 4.7.2)
- unmittelbare Prüfung von Pflichtfeldern, Formaten und fachlichen Plausibilitäten

- Upload von Nachweisen, Dokumenten und Bildern inkl. Prüfung von Dateityp, Dateigröße und Schadsoftware
- verständliche Fehlermeldungen und barrierefreie Fehlerführung
- Zusammenfassung und Korrekturmöglichkeit vor dem Absenden
- rechtssichere Erfassung und Versionierung notwendiger Erklärungen (z. B. Einwilligungen)
- eindeutige Eingangsbestätigung mit Vorgangsnummer, Information zum weiteren Bearbeitungsablauf sowie Statusanzeige, sofern die angebundenen KKH-Systeme entsprechende Informationen bereitstellen.

Die allgemeinen Anforderungen an Barrierefreiheit (Abschnitt 4.6) sowie an Datenschutz, Sozialdatenschutz, Löschkonzept und Datenspeicherung (Abschnitt 4.7) gelten für Formulare und den Online-Beitritt gleichermaßen. Speziell für den Online-Beitritt gelten darüber hinaus:

- transparente Datenschutzinformationen innerhalb der Antragsstrecke
- getrennte Erfassung optionaler Einwilligungen (z. B. für Werbung); keine Kopplung freiwilliger Werbeeinwilligungen an den Online-Beitritt
- keine Nutzung der Formulardaten für eigene Zwecke des Auftragnehmers, insbesondere nicht für Werbung, Profilbildung oder das Training von KI-Systemen
- keine personenbezogenen oder sozialen Daten in URLs, Tracking-Systemen oder Analysewerkzeugen

E-Mail-Routing

Für allgemeine Formulare muss ein regelbasiertes Routing nach Thema, Region und Zuständigkeit möglich sein. Dabei gelten folgende Vorgaben:

- transaktionale E-Mail-Zustellung über ein freigegebenes SMTP-Relay, abgesichert durch SPF/DKIM
- keine Übermittlung von Sozialdaten, Gesundheitsdaten oder Formulardokumenten per unverschlüsselter E-Mail; E-Mails enthalten grundsätzlich nur neutrale Eingangs- oder Bearbeitungshinweise, sensible Inhalte werden ausschließlich über freigegebene Systeme und Schnittstellen bereitgestellt
- Ende-zu-Ende-Verschlüsselung (TLS) bei der Datenübertragung sowie Verschlüsselung gespeicherter Formulardaten und Uploads
- CSRF-Schutz sowie Schutz vor XSS, Injection-Angriffen und automatisierten Angriffen
- Honey-pot-Felder sowie ein datenschutzkonformes, barrierefreies CAPTCHA (aktuell Friendly Captcha)
- Viren- und Schadsoftwareprüfung sämtlicher Uploads
- Privacy by Design: keine unnötige Speicherung sensibler Formulardaten, direkte Weiterleitung an KKH-Backend-Systeme wo möglich, Löschung nach den Vorgaben des Löschkonzepts (vgl. Abschnitt 4.7.2)
- Messung von Formularstart, Schritten, Abbrüchen, Fehlern und erfolgreichem Versand unter Berücksichtigung der Einwilligung aus dem Consent-Manager, ohne Übertragung von Feldinhalten oder Sozialdaten an Analyse- und Werbesysteme

- Übergabe freigegebener Kampagnenkennungen
- technische Unterscheidung zwischen Antragseingang und bestätigter Mitgliedschaft sowie Möglichkeit zur Messung des Prozesses bis zur Neuaufnahme
- keine Beeinträchtigung des Online-Beitritts bei abgelehntem Marketing- oder Analyse-Consent

4.3.13 Öffentliche Zustellung

Als Körperschaft des öffentlichen Rechts stellt die KKH amtliche Mitteilungen und Bescheide digital auf der Website öffentlich zu. Das CMS muss hierfür eine rechtssichere, barrierefreie und weitgehend automatisierte Verwaltung und Darstellung von PDF-Dokumenten bereitstellen.

a) Funktionale Anforderungen

Dateiverwaltung und DAM-Struktur:

- Strukturierte Ablage im DAM mit tagsweiser Untergliederung (Ordner 1–31), um auch bei sehr hohen Dateivolumina (mehrere Tausend PDFs) eine performante Verarbeitung zu gewährleisten
- Automatisches Auslesen und Taggen von Dateiattributen beim Upload (z. B. Zuordnung zum Anfangsbuchstaben des Adressaten)

Zeitsteuerung und Fristen (21-Tage-Zyklus):

- Automatisierte Steuerung von Veröffentlichungs- (OnTime) und Deaktivierungszeitpunkten (OffTime)
- Standardmäßige Publikationsdauer von 21 Tagen ab dem Folgetag der Einstellung (mit automatischer Veröffentlichung und Replikation um 0:05 Uhr)

Frontend-Darstellung (Akkordeon-Struktur):

- Übersichtliche und barrierefreie Darstellung auf einer dedizierten Unterseite.
- Dynamische Akkordeon-Struktur über drei Ebenen:
 1. Kalenderwoche
 2. Datum
 3. Alphabetische Gruppen (z. B. A–G, H–P, Q–Z) mit den jeweiligen PDF-Downloads
- Performance-optimiertes Nachladen der Inhalte beim Aufklappen der einzelnen Buchstabensegmente

Automatisierter Lösch- und Archivierungs-Job:

Nächtlicher Hintergrundprozess (z. B. um 00:10 Uhr), der:

1. Alle PDFs aus dem DAM löscht, deren Aushangsfrist (> 21 Tage) abgelaufen ist
2. Automatisch ein zusammenfassendes Log-PDF im Archiv-Ordner erzeugt, das alle am jeweiligen Tag aktuell aktiven Zustellungen protokolliert

3. Den Seiten-Cache auf den Live-Systemen automatisch leert, damit abgelaufene Dokumente sofort verschwinden

b) Rechtliche und nicht-funktionale Anforderungen

Rechtssicherheit und Audit-Trail: Nachweisbarkeit der ordnungsgemäßen Veröffentlichung durch das automatisiert erzeugte Tages-Log-PDF im Archiv.

Datenschutz und SEO-Steuerung: Gezielter Ausschluss der Unterseite und der PDFs von der Indexierung durch externe Suchmaschinen (z. B. per noindex, nofollow), um den Schutz personenbezogener Daten nach Ablauf der Frist zu gewährleisten.

Barrierefreiheit: Vollständige Einhaltung der Vorgaben nach BITV 2.0/WCAG 2.2 AA für die Webkomponente sowie die bereitgestellten Dokumente.

4.3.14 Weiterführende CMS-Funktionen

Weitere zusätzliche Funktionalitäten sind nicht zwingend erforderlich, diese werden jedoch im Kriterienkatalog positiv bewertet:

- LLMO-Optimierungsmöglichkeiten
- Erweitertes Monitoring/Page-Health-Report (z. B. für Formulare, E-Mail-Routing, tote Links)
- Innovationsfähigkeit für zukünftige Themen wie Personalisierung, Chatbots und weitere KI-gestützte Funktionen

4.4 Anforderungen an Betrieb und technische Architektur

4.4.1 Zielarchitektur

Die Plattform ist als skalierbare, containerisierte Cloud-native Architektur zu konzipieren.

- CMS/Backend: Enterprise-CMS (z. B. TYPO3) in vollständig containerisierter Umgebung (Docker/Kubernetes)
- Frontend: Komponenten-basiertes Frontend (HTML5, CSS3, JavaScript; optional React/Next.js für interaktive Bereiche)
- Datenhaltung: MariaDB/MySQL für CMS-Daten, Redis für Session- und Cache-Management, S3-kompatibles Object Storage
- Schnittstellen-Layer: Definierte REST-API-Schicht für alle Drittdienst-Integrationen; API-Gateway mit Rate-Limiting

- Sicherheits-Layer: WAF (OWASP ModSecurity CRS), DDoS-Schutz, HTTPS/TLS 1.3, HSTS, Content Security Policy
- CI/CD: Vollautomatisierte Build-, Test- und Deployment-Pipelines (GitLab CI/CD oder vergleichbar)
- Physische Resilienz und Krisenvorsorge: Die Anforderungen aus dem KRITIS-Dachgesetz sind zu berücksichtigen, insbesondere hinsichtlich physischer Resilienz der Rechenzentren, Stromversorgung, redundanter Kommunikation, Zutrittsschutz und Krisenvorsorge.

4.4.2 Umgebungskonzept

Für alle Projekte ist eine durchgängige Multi-Environment-Architektur verbindlich:

Folgende Mindestanforderungen sind:

- Entwicklungsumgebung (DEV): Lokale oder serverbasierte Umgebung für Entwickler
- Test-/QA-Umgebung (TEST): Dedizierte Umgebung für interne Qualitätssicherung und automatisierte Tests
- Produktionsumgebung (LIVE): Ausschließlich freigegebene Änderungen über die CI/CD-Pipeline, kein Direkt-Deployment

Weitere zusätzliche Funktionalitäten sind nicht zwingend erforderlich, diese werden jedoch im Kriterienkatalog positiv bewertet:

- Staging-Umgebung (STAGING): Produktionsnahe Umgebung für fachliche Abnahme; technisch identisch mit Live

4.4.3 Deployment-Prozess

Folgende Mindestanforderungen sind:

- Stufenmodell: Build → automatisierte Unit-, Integrations- und E2E-Tests → Security-Scans → Deployment
- SAST-, DAST- und Dependency-Scans sind verbindliche Mindestanforderung sowie Security-Gate vor jedem Produktivdeployment
- Verbindliches Software-Supply-Chain-Management, einschließlich SBOM, CVE-Monitoring, EOL/EOS-Management, Dependency-Management und nachvollziehbarer Build-Artefakte

Weitere zusätzliche Funktionalitäten sind nicht zwingend erforderlich, diese werden jedoch im Kriterienkatalog positiv bewertet:

- Commit-basiertes Triggering bei Merge in definierte Branches
- Statistische Code-Analyse als Qualitäts-Gate vor Merge

- Approval-Gates für Produktions-Deployments (4-Augen-Prinzip)
- Zero-Downtime-Deployments (Rolling Updates oder Blue-Green)
- Automatisierter Rollback auf vorherige stabile Version
- Manuelle Eingriffe auf der Produktionsumgebung sind ausgeschlossen

4.4.4 Monitoring, Logging und Alerting

Der Auftragnehmer hat ein vollständiges Monitoring- und Logging-Konzept zu implementieren:

- Infrastruktur-Monitoring (CPU, RAM, Disk, Network) mit Echtzeit-Dashboards
- Application-Monitoring (Sentry oder vergleichbar) für Exceptions und Performance
- Uptime-Monitoring für alle Endpunkte
- Zentralisiertes Logging (ELK-Stack oder Grafana Loki); Aufbewahrung mindestens 6 Monate
- Anonymisierung personenbezogener Daten in Logs vor der Protokollierung
- WAF-Monitoring mit automatisierter Meldung bei Anomalien
- Mehrstufiges Alert-Routing (E-Mail, SMS/Telefon für P1) an definierte On-Call-Personen
- Möglichkeit zur SOC-Integration der KKH bei sicherheitsrelevanten Ereignissen

Angriffserkennung

Die Monitoring-, WAF-, Logging- und SOC-Anforderungen sind ausdrücklich als Bestandteil eines Systems zur Angriffserkennung gemäß § 31 BSIG auszugestalten, einschließlich kontinuierlicher Auswertung und definierter Security-Alarmierung.

Security-Incident-Meldeprozess

Der Auftragnehmer hat einen verbindlichen Security-Incident-Meldeprozess an die KKH aufzunehmen. Dieser muss die gesetzlichen Meldefristen nach BSIG und DSGVO berücksichtigen und der KKH ausreichend Vorlauf für ihre eigenen Meldungen ermöglichen. Die Meldezeiten des Auftragnehmers sind vertraglich verbindlich festzulegen (vgl. Abschnitt 4.7.4).

4.4.5 Zertifikate

Der Auftragnehmer übernimmt im Rahmen der Domainverwaltung die Beschaffung, Implementierung und laufende Pflege aller für den ordnungsgemäßen und sicheren Betrieb von kkh.de erforderlichen SSL/TLS-Zertifikate (mindestens TLS v1.2 oder höher).

Die konkrete Liste der zum Zeitpunkt der Leistungsaufnahme aktiven kkh.de-Subdomains und zugehörigen Zertifikate wird dem Auftragnehmer im Rahmen der Übergabe nach Zuschlagserteilung mitgeteilt.

4.5 Anforderungen an Content-Migration

Die Migration umfasst neben www.kkh.de auch das unter arztlotse.kkh.de betriebene Angebot „Arztlotse“, das in die neue Systemumgebung zu überführen ist. Die Migration aus dem bestehenden System (Adobe Experience Manager) ist strukturiert und mehrstufig durchzuführen. Folgende Prozessschritte sind verbindlich:

- Vollständige Bestandsaufnahme (Content-Inventory) aller Seiten, Inhaltstypen, Assets und Metadaten
- Analyse der AEM-Struktur: Seitentypen, Inhaltsmodelle, Templates, Custom-Komponenten, DAM-Assets
- Mapping der Altsystem-Strukturen auf die Zielarchitektur des neuen CMS
- Entwicklung und Durchführung automatisierter Migrationsskripte für strukturierte Inhalte
- Manuelle Veredelung strategisch relevanter Inhalte sowie solcher, deren Struktur sich im neuen System grundlegend ändert
- Asset-Migration aller Medien (Bilder, Dokumente, Videos) mit Erhalt der Metadaten
- Lückenloses Redirect-Mapping: Alle bestehenden URLs erhalten 301-Weiterleitungen zur Sicherung der SEO-Rankings
- Qualitätssicherung: Automatisierter Abgleich (Vollständigkeit, Korrektheit) sowie stichprobenartige Sichtprüfung

Hinweis zur Migrationstiefe: Welche Inhalte vollständig automatisiert und welche manuell migriert werden, ist gemeinsam mit der KKH in der Konzeptionsphase festzulegen. Nicht strukturierte oder veraltete Inhalte können einer Überarbeitung bedürfen, die im Rahmen der Migrationsstrategie gesondert zu bewerten sind.

4.6 Anforderungen an Barrierefreiheit und Nutzerorientierung

4.6.1 Anforderungen an Barrierefreiheit

Barrierefreiheit ist keine optionale Anforderung, sondern gesetzliche Verpflichtung und Qualitätsmerkmal. Der Auftragnehmer muss umfassende Erfahrung in der Umsetzung barrierefreier Webprojekte nachweisen. Alle Leistungen sind konform mit:

- BITV 2.0

- WCAG 2.2 Level AA als verbindlicher Mindeststandard
- EN 301 549 (europäische Norm für digitale Barrierefreiheit)

Barrierefreiheit ist als Accessibility by Design von der ersten Konzeptionsphase an in alle Projektstufen zu integrieren:

- Konzeption/UX: Ausreichende Kontrastverhältnisse, skalierbare Schriftgrößen, keine rein farbbasierte Informationsvermittlung, logische Navigationsstruktur
- Entwicklung: Semantisches HTML5, ARIA-Rollen und -Attribute, vollständige Tastaturbedienbarkeit, barrierefreie Formulare
- Testing: Automatisierte Prüfungen (z.B. axe DevTools, Lighthouse, WAVE, Pa11y) in der CI/CD-Pipeline sowie manuelle Tests mit Screenreadern (z.B. NVDA, JAWS, VoiceOver) als reguläre Qualitätssicherung
- Schulungen für Mitarbeiter des Auftraggebers in barrierefreier Inhaltspflege; CMS-seitige Unterstützung, z. B. Pflichtfelder für Alternativtext (s. auch Kapitel 8.2 Schulungsangebote)

4.6.2 Barrierefreiheit im laufenden Betrieb

Die Barrierefreiheit ist auch im laufenden Betrieb dauerhaft sicherzustellen:

- Accessibility-Scans bei jedem Deployment
- Regelmäßige Scans des gesamten Live-Auftritts
- Periodische manuelle Audits bei größeren Releases
- Feedback-Mechanismus auf der Website für Nutzer-Meldungen (Pflicht gemäß BITV 2.0)
- Unterstützung bei der jährlichen Aktualisierung der Barrierefreiheitserklärung gemäß § 12 BGG
- Unterstützung bei externen Prüfungen zur Barrierefreiheit, z.B. durch die Überwachungsstelle des Bundes

4.6.3 Mobile-First

Mobile First ist als methodische Grundlage für Konzeption, Design und Entwicklung verbindlich. Die Umsetzung umfasst:

- UX-Konzeption startet mit mobilen Breakpoints und wird auf größere Bildschirmformate erweitert
- Touch-Optimierung: Ausreichend große Touch-Targets (mind. 44×44 px), keine reinen Hover-Interaktionen

- Performance-Optimierung für mobile Netzwerke (Bilder-Komprimierung, Lazy Loading, minimale JS-Bundles)
- Core Web Vitals (LCP, CLS, INP): Zielwert 'Good' in Google PageSpeed Insights auf mobilem Gerät
- Testing auf echten mobilen Endgeräten (iOS und Android) in verschiedenen Auflösungen
- Cross-Browser-Testing (mind. aktuelle Versionen der marktrelevanten desktop-Browser)

4.7 Anforderungen an IT-Sicherheit und Datenschutz

Die Verarbeitung personenbezogener und sozialer Daten muss den geltenden gesetzlichen Vorgaben entsprechen. Maßgeblich sind insbesondere die DSGVO, das BDSG, das Sozialgeheimnis nach § 35 SGB I sowie die Regelungen zum Sozialdatenschutz nach §§ 67 ff. SGB X. Für die Beauftragung von Dienstleistern gelten die Vorgaben zur Auftragsverarbeitung nach § 80 SGB X, einschließlich der dort geregelten Anzeige- und Vertragsanforderungen gegenüber externen Dienstleistern mit Zugriff auf Sozialdaten. Nach § 392 SGB V sind Krankenkassen zu Maßnahmen nach dem Stand der Technik verpflichtet. Der branchenspezifische Sicherheitsstandard B3S-GKV/PV gilt in der jeweils gültigen Fassung als verbindliche Mindestanforderung. Diese Verpflichtung ist auf alle relevanten Unterauftragnehmer durchzureichen. Diese Anforderungen sind vertraglich auch gegenüber beteiligten IT-Dienstleistern abzusichern.

4.7.1 Compliance mit KKH Security-Guides für digitale Services

Der Auftragnehmer hat die Dokumente „Anlage – Anforderungen IT-Security“ (als Ergänzung der Allgemeinen Rahmenbedingungen IT-Service Management) sowie „Anlage - IT-Security-Guide (Auszug Web-Infrastruktur)“ vollständig zu sichten und ihre Einhaltung im Rahmen der Angebotsphase im Kriterienkatalog zu bestätigen.

4.7.2 Löschkonzept und Aufbewahrungsfristen

Der Auftragnehmer hat ein Löschkonzept vorzulegen, das den gesamten Lebenszyklus personenbezogener Daten auf der Plattform abdeckt. Dazu zählen beispielsweise:

- Dokumentation aller verarbeiteten Datenkategorien und der jeweils zugehörigen Aufbewahrungsfristen (u. a. Formulardaten, Kontaktanfragen, Logdaten, Cookie-/Consent-Daten)
- Klare Regelung des Umgangs mit Daten aus Online-Formularen: fristgerechte, automatisierte Löschung nach Zweckerfüllung bzw. direkte Weiterleitung an KKH-Backend-Systeme ohne dauerhafte Speicherung im CMS (vgl. Abschnitt 4.3.12)

- Technische Umsetzung automatisierter Löschroutinen (Data-Retention-Jobs) inkl. Protokollierung der Löschvorgänge

4.7.3 Datenspeicherung und -verarbeitung

Alle Daten sind ausschließlich innerhalb der Europäischen Union, bevorzugt in Deutschland, zu verarbeiten und zu speichern. US-Hyperscaler sind als primäre Hosting-Plattform ausgeschlossen. Für die Verarbeitung von Sozialdaten gemäß SGB V ist besondere Sorgfalt anzuwenden (§§ 67 ff. SGB X). Alle eingesetzten Drittdienste sind auf EU-konformes Hosting zu prüfen.

Bei Nutzung von Cloud-Diensten sind zusätzlich die gesetzlichen Vorgaben nach § 393 SGB V zur Verarbeitung von Sozial- und Gesundheitsdaten in der Cloud zu erfüllen. Hierzu zählen insbesondere ein zulässiger Verarbeitungsstandort, die Niederlassung der datenverarbeitenden Stelle in Deutschland sowie ein aktuelles C5-Typ-2-Testat gemäß § 393 SGB V oder die Vorlage eines Maßnahmenplanes inkl. Meilensteinplanung, der vorsieht innerhalb von 24 Monaten ab Erstellung des Maßnahmenplanes ein C5-Typ2-Testat zu erhalten. Sofern Cloud-Dienste zum Einsatz kommen, sind diese Vorgaben vom Hosting-Anbieter (auch als Unterauftragnehmer) ebenfalls zu erfüllen und nachzuweisen. Der für die Leistung relevante Scope des Testats ist einzubeziehen und nachzuweisen. Ein nachweislich vergleichbarer bzw. höherwertiger Sicherheitsstandard kann nur nach Abstimmung mit der KKH anerkannt werden. Neben dem Hosting sind auch Administrations-, Support-, Telemetrie-, Backup- und sonstige Fernzugriffe sowie sämtliche Unterauftragnehmer hinsichtlich Standort, Sozialdatenschutz und Zugriffsmöglichkeiten verbindlich zu regeln. Die Anforderungen an EU-Verarbeitung und Auftragsverarbeitungsverträge nach Abschnitt 5 gelten entsprechend.

4.7.4 Wartung/Support/Service etc.

Der Auftragnehmer hat das Dokument „Anlage -Allgemeine Rahmenbedingungen IT Service Management V3.0“ inkl. des ergänzenden Dokuments „Anlage – Anforderungen IT-Security“ vollständig zu sichten und ihre grundsätzliche Einhaltung im Rahmen der Angebotsphase im Kriterienkatalog zu bestätigen.

IT-forensische Unterstützung und Beweissicherung

Der Auftragnehmer hat die KKH bei Sicherheitsvorfällen IT-forensisch zu unterstützen und Beweise zu sichern. Dazu gehören insbesondere Log-Sicherung, Zeitstempelsynchronisation, Chain of Custody, Indicators of Compromise (IoCs), Root-Cause-Analyse und Unterstützung bei aufsichtsrechtlichen Verfahren.

4.7.5 Schutzbedarfs- und KRITIS-Scope-Bewertung

Der Auftragnehmer hat eine dokumentierte Schutzbedarfs- und KRITIS-Scope-Bewertung für Website, Arztlotse, Online-Beitritt, öffentliche Zustellung, APIs und Betriebsinfrastruktur vorzulegen.

4.7.6 Risikoanalyse

Der Auftragnehmer hat eine dokumentierte Risikoanalyse nach § 30 BSIG, BSI-Standard 200-3 und ISO/IEC 27001 vorzulegen. Sie umfasst Risikoregister, Maßnahmen, Restrisiken und formale Risikoakzeptanz. Die Analyse ist vor Go-Live und bei wesentlichen Änderungen zu erstellen bzw. fortzuschreiben.

4.7.7 Audit-, Kontroll- und Nachweisrechte

Der KKH stehen verbindliche Audit-, Kontroll- und Nachweisrechte zu. Diese umfassen C5-Berichte, relevante Zertifizierungsnachweise, Pentest-Berichte und Maßnahmenpläne sowie die Unterstützung bei Prüfungen nach § 39 BSIG.

4.8 Anforderungen an SEO und Generative Engine Optimization (GEO/LLMO)

4.8.1 Technische SEO-Grundlage (Crawling & Indexierung)

Weitere zusätzliche Funktionalitäten sind nicht zwingend erforderlich, diese werden jedoch im Kriterienkatalog positiv bewertet:

- Saubere URL-Strukturen ohne dynamische Parameter
- Meta-Robots-Tags pro Seite/Content-Objekt konfigurierbar (mindestens index/noin-index und follow/nofollow), inkl. konfigurierbarem Standardverhalten
- Steuerbare, gültige robots.txt (im CMS oder über zentrale Konfigurationsdatei pflegbar); Staging-/Testumgebungen können über Disallow oder Passwortschutz vom Index ausgeschlossen werden
- Automatisch generierte XML-Sitemaps für alle indexierbaren Inhaltstypen (Seiten, Blog, Kategorien etc.); automatische Aktualisierung bei Content-Änderungen, automatisches Splitting bei mehr als 50.000 URLs, Aufnahme nur indexierbarer Seiten (kein noindex, 30x, 404)
- Canonical-Tags pro Seite (Standard: selbstreferenzierend), zusätzlich individuell konfigurierbares Canonical-Ziel
- Hreflang-Tags pro Seite für mehrsprachige/länderspezifische Inhalte, inkl. Rückverweisen und optionalem x-default

- Schema.org-Markup (JSON-LD) für relevante Inhaltstypen (Organisation, FAQPage, Breadcrumb, MedicalOrganization)
- Server-Side Rendering (SSR) für SEO-kritische Inhalte
- Core Web Vitals als Development-Qualitätskriterium (Lighthouse in CI/CD integriert)
- Bildoptimierung (WebP, AVIF, responsive Images mit srcset/sizes)
- Log-File-Analyse und regelmäßige Crawl-Analyse (Screaming Frog, Google Search Console)

4.8.2 On-Page-SEO und Metadaten

Weitere zusätzliche Funktionalitäten sind nicht zwingend erforderlich, diese werden jedoch im Kriterienkatalog positiv bewertet:

- Eigenständiger, pro Seite editierbarer Title-Tag mit konfigurierbarem Standard-Template (z. B. „Seitentitel | KKH“)
- Pro Seite editierbare Meta-Description mit Anzeige der Zeichenanzahl (z. B. 0 bis 160 Zeichen) und optionalem Standard-Template
- Open-Graph-/Social-Meta-Daten pro Seite (OG-Titel, OG-Beschreibung, OG-Bild) mit sinnvoller Fallback-Logik aus SEO-Titel/-Description/-Bild
- Saubere, hierarchische Überschriftenstruktur (H1 bis H6): genau eine H1 pro Seite, keine zweckentfremdete Nutzung von H-Tags für Layoutzwecke
- Pflicht zur Hinterlegung von Alt-Texten pro Bild, sinnvolle Bilddateinamen sowie Lazy Loading als Standard im nicht sichtbaren Bereich
- Komfortable interne Verlinkung über eine integrierte Seitensuche im Link-Dialog (keine manuelle URL-Eingabe), mit frei editierbarem Ankertext
- Breadcrumb-Navigation, die die Position einer Seite konsistent entlang der logischen Hierarchie abbildet

4.8.3 URL-Struktur, Weiterleitungen und Systemseiten

Für eine stabile, suchmaschinenfreundliche URL- und Fehlerbehandlung gelten folgende Mindestanforderungen:

- Sprechende, SEO-freundliche Permalinks auf Basis von Slugs/Titeln ohne technische IDs in der sichtbaren URL; je Inhaltstyp konfigurierbare URL-Muster, manuell editierbare Slugs, sinnvolle Transliteration von Umlauten und Sonderzeichen
- Konsistente Domain- und Protokollregeln: einheitliche Auslieferung per HTTPS, erzwingene eindeutige Domainvariante (mit/ohne www) sowie einheitlicher Umgang mit abschließendem Slash, jeweils per 301 durchgesetzt

- Integrierter Redirect-Manager für 301-Weiterleitungen mit Übersicht (alte URL → neue URL, Statuscode), redaktioneller Pflege ohne Entwicklerunterstützung und automatischer Erzeugung bei Slug-/URL-Änderungen; keine Redirect-Ketten
- Individuelle 404-Seite mit korrektem HTTP-Statuscode 404 sowie hilfreichen Links bzw. Suche
- Staging- und Wartungsumgebungen dürfen nicht indexiert werden (Authentifizierung und/oder globale noindex-Signale); eindeutige Trennung von Live- und Staging-Domain
- Vollständige Auslieferung über HTTPS ohne Mixed-Content (keine HTTP-Ressourcen auf HTTPS-Seiten)

4.8.4 SEO-sicherer Relaunch

Der Relaunch ist mit einem strukturierten SEO-Schutzkonzept durchzuführen, um Sichtbarkeitsverluste zu minimieren:

- Vollständiger Crawl des Altsystems vor Relaunch: Inventarisierung aller URLs, Rankings, organischer Traffic-Quellen und Backlinks
- Systematisches 1:1-Redirect-Mapping aller relevanten Alt-URLs (301-Weiterleitungen ohne Redirect-Chains)
- Erhalt bewährter URL-Strukturen wo immer möglich
- Umfassende technische SEO-Prüfung auf der Staging-Umgebung vor Go-Live
- Intensiviertes Post-Relaunch-Monitoring in den ersten 4 bis 8 Wochen (Google Search Console, Ranking-Tools, Traffic-Analyse)
- Sofortige Reaktionsfähigkeit bei unerwarteten Sichtbarkeitsverlusten

4.8.6 Analytics, Tracking und Search Console

Das CMS muss folgende Mindestanforderungen an Tracking und Verifizierung erfüllen:

- Einbindung von Tracking-Skripten (z. B. Google Tag Manager) über einen zentralen Einstellungsbereich (Head/Body), ohne manuelle Template-Änderungen
- Pflege von Verifizierungs-Meta-Tags (z. B. Google Search Console, Bing) über das Backend
- Sämtliche Tracking-Skripte sind technisch mit dem Consent-Management nach § 25 TDDDG und DSGVO zu koppeln. Nicht erforderliche Zugriffe auf Endgeräte dürfen erst nach wirksamer Einwilligung erfolgen.

4.8.7 Optimierung für KI-gestützte Systeme (LLMO/GEO)

Inhalte sind so aufzubereiten, dass sie nicht nur von klassischen Suchmaschinen, sondern auch von KI-gestützten Such- und Antwortsystemen (Large Language Models, KI-Assistenten) gefunden, verstanden und als verlässliche Quelle genutzt werden können:

- Umfangreiches Schema.org-Markup als Kontext-Signal für KI-Systeme
- Klare semantische HTML-Struktur; deutlich gekennzeichnete Autorschaft und Aktualität
- Strukturierte Inhalte mit klaren Antworten auf häufige Nutzerfragen (FAQ-Format)
- API-Zugänglichkeit für KI-Systeme (RAG-fähige Schnittstellen)
- llms.txt als emerging Standard für KI-Agenten-Guidance
- Monitoring der Präsenz von kkh.de in KI-generierten Antworten
- Datenschutz: Sicherstellung, dass keine personenbezogenen Daten in KI-Trainingsdaten einfließen
- KI-Governance nach EU AI Act für zukünftige produktive KI-Funktionen, insbesondere Klassifizierung, Datenschutz- und Security-Prüfung, Human Oversight, Dokumentation und AI-Literacy

4.8.8 Erweiterte SEO-Funktionen (Optional)

Weitere zusätzliche Funktionalitäten sind nicht zwingend erforderlich, diese werden jedoch im Kriterienkatalog positiv bewertet:

- Massенbearbeitung von SEO-Feldern (Title, Description, Indexierungsflags) in einer Listenansicht
- Template-Engine für dynamische SEO-Titel und -Descriptions mit Platzhaltern
- Komfortabler JSON-LD-Editor/Mapper zur Zuordnung von CMS-Feldern zu Schema.org-Properties inkl. Validierung
- SEO-Qualitätsübersicht/Dashboard im Backend mit Hinweisen auf fehlende Titles, Descriptions, 404-Häufungen und Redirect-Ketten
- Erweiterte Vorschaufunktion mit Anzeige von Title, Meta-Description, Canonical, sozialer Vorschau und strukturierten Daten
- Rollen- und Freigabeprozesse speziell für SEO-Felder
- FAQ- und Glossar-Module mit optionalem FAQ-Schema und automatischer interner Verlinkung wichtiger Begriffe

4.9 Anforderungen an Zukunftsfähigkeit und Innovation

4.9.1 Integration neuer Technologien

Der Auftragnehmer muss neue technologische Entwicklungen kontrollieren und ohne Gefährdung von Stabilität und Sicherheit in die bestehende Plattform integrieren. Folgende Mindestanforderungen sind:

- Modulare, lose-gekoppelte Architektur (API-first) als Grundvoraussetzung für den sicheren Technologieaustausch
- Proof of Concept in isolierter Umgebung vor produktivem Einsatz jeder neuen Technologie
- Feature Flags für schrittweise Rollouts mit parallelem Monitoring
- Security-Review und Penetrationstest vor Integration in Produktion sowie für das Gesamtsystem vor Go-Live, nach wesentlichen Änderungen und regelmäßig im laufenden Betrieb
- Dokumentation aller Architekturentscheidungen inklusive verworfener Alternativen
- Sofortige Rollback-Fähigkeit bei unerwarteten Instabilitäten
- Bei Produkten mit digitalen Elementen: Nachweis der Konformität mit dem Cyber Resilience Act (CRA), Vulnerability Handling, Herstellersupport, Security Updates und, soweit anwendbar, SBOM bzw. Herstellerinformationen

5. Leistungsort/Lieferbedingungen

Das Hosting ist ausschließlich in EU-Rechenzentren, bevorzugt in Deutschland, zu realisieren. US-Hyperscaler (AWS, Azure, Google Cloud Platform) sind als primäre Hosting-Plattform ausgeschlossen. Empfohlene Partner sind: Plusserver, STACKIT, Open Telekom Cloud, Hetzner, IONOS.

Alle Auftragsverarbeitungsverträge (AVV) gemäß Art. 28 DSGVO sind vor Betriebsaufnahme abzuschließen.

Die Ausfallsicherheit ist gemäß KRITIS-Verordnung sicherzustellen (branchenspezifisch konkretisiert im B3S-GKV/PV des GKV-Spitzenverbands, vom BSI festgestellt am 09.04.2025). Die Wiederherstellung von Website-Versionen durch den Auftragnehmer muss jederzeit möglich sein (s. Anlage – IT-Security-Guide AUSZUG Web-Infrastruktur). Die Wiederherstellbarkeit ist durch folgende Mindestanforderungen nachzuweisen:

- messbare Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO)
- definierte Backup-Zyklen
- Verschlüsselung der Backups
- getrennte bzw. unveränderbare Backups

- regelmäßige Restore-Tests
- regelmäßige Notfallübungen

6. Schulungsangebote

Der Auftragnehmer hat ein praxiserprobtes Schulungskonzept vorzulegen und die Schulungen zielgruppengerecht durchzuführen. Zu allen Schulungsformaten sind aktuelle, leicht verständliche Schulungsunterlagen digital bereitzustellen.

Für die eindeutige Bepreisung im Preisblatt gelten folgende Leistungseinheiten und Mindestanforderungen:

a) Pflichtmodule (Kern-Schulungspaket)

CMS-Grundlagenschulung (Basisschulung):

- Format: Interaktiver Remote-Workshop (1 ganzer Tag / 8 Std.)
- Teilnehmerzahl: Max. 10 Personen pro Durchgang
- Inhalt: Bedienung des CMS, Navigationsstruktur, Anlegen von Standardseiten, Content-Elementen und Medienverwaltung.
- Abfrage im Preisblatt: Pauschalpreis pro Schulungsdurchgang

Rollenspezifische Spezialschulung (Erweiterte Workflows):

- Format: Remote-Workshop (0,5 Tage/4 Std.)
- Teilnehmerzahl: Max. 8 Personen pro Durchgang
- Inhalt: Freigabeprozesse (Vier-Augen-Prinzip), Rechte-/Rollenverwaltung, erweiterte Redaktionsfunktionen (z. B. Admin-Rechte).
- Abfrage im Preisblatt: Pauschalpreis pro Schulungsdurchgang

Spezialmodul „Barrierefreie Inhaltspflege“:

- Format: Remote-Workshop (0,5 Tage / 4 Std.)
- Teilnehmerzahl: Max. 10 Personen pro Durchgang
- Inhalt: Erstellung barrierefreier Webinhalte nach BITV 2. /WCAG 2.2 AA (z. B. Alt-Texte, semantische Überschriften, barrierefreie Linktexte und PDF-Einbindung).
- Abfrage im Preisblatt: Pauschalpreis pro Schulungsdurchgang

Redakteur-Handbuch und Systemdokumentation:

- Format: Vollständige, strukturierte Dokumentation in Confluence/CMS inklusive Anleitungen für Standard-Arbeitsabläufe
- Abfrage im Preisblatt: Pauschalpreis (Einmalaufwand)

b) Optionale Schulungsleistungen (Abruf nach Bedarf)

- Video-Tutorials/Screen-Recordings:
 - Format: Kurze, vertonte Video-Anleitungen (Micro-Learnings, ca. 2 bis 5 Minuten) für wiederkehrende Standardaufgaben
- Abfrage im Preisblatt: Pauschalpreis pro Video-Tutorial

Auffrischungsschulungen & Individual-Trainings:

- Format: Zielgruppenorientierte Schulung bei größeren System-Updates, neuen Features oder für neue Mitarbeitende (Remote)
- Abfrage im Preisblatt: Stundensatz

7. Dokumentation und Übergabe bei Vertragsende

Der Auftragnehmer hat nach Umsetzung der fachlichen Anforderungen sowie zum Ende der Vertragslaufzeit eine umfangreiche und aktuelle Dokumentation aller Funktionalitäten der Website in Form eines Handbuches zu erstellen und der KKH zu überlassen. Die Dokumentation muss in deutscher Sprache erfolgen und darf in elektronischer Form zur Verfügung gestellt werden.

Die Dokumentation umfasst:

- eine Übersicht über alle für den reibungslosen Betrieb relevanten Arbeitsschritte zur Bedienung und Nutzung der einzelnen Funktionalitäten
- eine Dokumentation der fachlichen Prozesse (wie Workflow-Beschreibung oder Upload-Verfahren)
- eine Auflistung aller relevanten Verlinkungen und Zugänge (z. B. Testserver)
- eine vollständige Abschlusssdokumentation zum Ende der Vertragslaufzeit, die alle für eine nahtlose Übergabe an die KKH oder einen Nachfolgeauftragnehmer erforderlichen Informationen, technischen Architekturen und Betriebsdokumentationen enthält
- eine vollständige Übergabe und Dokumentation aller Zugänge, Zugangsdaten, Repositories, Lizenzen, Zertifikate und administrative Konten (inkl. Haupt- und Testsystem) im Eigentum bzw. Verantwortungsbereich der KKH
- eine aktuelle Übersicht der technischen Systemlandschaft, aller eingesetzten Skripte, Schnittstellen (APIs), Drittanbieter-Integrationen sowie der System- und Serverkonfigurationen