Leistungsbeschreibung zum Vergabeverfahren

Unterstützung für die Weiterentwicklung und den Betrieb von Softwareindividuallösungen

Inhaltsverzeichnis

Leistungsbeschreibung zum Vergabeverfahren 1
Unterstützung für die Weiterentwicklung und den Betrieb von Softwareindividuallösungen 1
Inhaltsverzeichnis 2
1.1 Einordung des Vergabeverfahrens 4
1.2 Inhalt des Vergabeverfahrens / Auftragsgegenstand 4
1.3 Leistungsabgrenzung zu bestehenden IT-Verträgen 5
1.4 Zeitlicher Überblick 5
1.5 Auftragsvolumen 6
1.6 Ort der Leistungserbringung 6
2 Anforderungen aus dem Rahmenvertrag 7
2.1 SBK-spezifische Informationen 7
2.2 Anforderungen an die Zusammenarbeit 7
2.2.1 Zentraler Ansprechpartner (Key Account Manager) 7
2.2.2 Verfügbarkeit zentraler Ansprechpartner 8
2.2.3 Auftrags- und Vertragssprache 8
2.2.4 Nearshoring im Europäischen Wirtschaftsraum (EWR) 8
2.2.5 Leitplanken der Zusammenarbeit 8
2.2.6 Qualitätsmanagement 9
2.3 Anforderungen an die Bieterunternehmen 10
2.3.1 Zertifizierungen 10
2.3.2 IT-Sicherheit 10
2.3.3 KRITIS und branchenspezifische Sicherheitsanforderungen 12
2.3.4 Einsatz von KI-/LLM-gestützten Werkzeugen 13
2.4 Anforderungen an Projektrollen und Erfahrungsklassen 15
2.4.1 Allgemeine Kenntnisse und Fähigkeiten 15
2.4.2 Business Analyst (Senior) 16
2.4.3 Business Analyst (Professional) 16
2.4.4 IT-Projektmanager (Senior) 16
2.4.5 IT-Projektmanager (Professional) 16
2.4.6 Software- / Lösungsarchitekt (Senior) 17
2.4.7 Java Full Stack Software Entwickler (Senior) 17
2.4.8 Java Full Stack Software Entwickler (Professional) 17
2.4.9 Java Full Stack Software Entwickler (Junior) 17
2.4.10 Platform- / DevOps Engineer (Senior) 17
2.4.11 IT-Betriebsspezialist (Senior) 18

2.4.12 IT-Betriebsspezialist (Professional) 18
2.4.13 IT-Betriebsspezialist (Junior) 18
2.4.14 Regressionstester (Junior) 18
2.5 Leistungsarten und leistungsartspezifische Anforderungen 20
2.5.1 Business Analyse und Requirements Engineering 20
2.5.2 Projektmanagement und Projektleitung 20
2.5.3 Softwaredesign / -architektur 20
2.5.4 Softwareentwicklung 20
2.5.5 Testmanagement 23
2.5.6 Integration / Deployment / Migration 24
2.5.7 Applikationsbetrieb und –support 25
2.5.8 Beratung zu den Fachgebieten Softwareentwicklung, -architektur und Applikationsbetrieb 26

Allgemeine Übersicht

1.1 Einordung des Vergabeverfahrens

Die SBK versichert mehr als eine Million Menschen und beschäftigt rund 2.000 Mitarbeiter. Als gesetzliche Krankenkasse arbeitet sie in einem besonders regulierten Umfeld mit hohen Anforderungen an Datenschutz, Informationssicherheit, Wirtschaftlichkeit, Nachhaltigkeit, Nachweisfähigkeit und betriebliche Resilienz.

Im Fokus des Kostenbewusstseins stehen die IT-Kosten-Transparenz, effiziente Prozesse, die fortlaufende Optimierung der eingesetzten Technologien sowie die Hebung neuer Potenziale durch Innovation. Wirtschaftliches Handeln bedeutet für die IT-Organisation insbesondere auch, die Geschäftsprozesse - und damit die Anwender - optimal zu unterstützen. Die Prozesse müssen sich hinsichtlich Effektivität und Effizienz daran ausrichten.

Von den zukünftigen Dienstleistern *(im Folgenden: Auftragnehmer)* wird erwartet, dass die SBK mit allen hier ausgeschriebenen Leistungen umfassend, effizient und professionell unterstützt wird. Die SBK ist dabei besonders am Aufbau einer kooperativen Zusammenarbeit mit den Auftragnehmern interessiert. Diese soll nachhaltig dazu beitragen, dass die SBK ihre angestrebten strategischen Ziele Kundenbegeisterung, qualitatives Wachstum, finanzielle Stabilität, engagierte Mitarbeiter sowie nutzerzentriertes und proaktives IT- und Datenmanagement erreicht. Die Auftragnehmer sind daher auch angehalten, der SBK im Kontext aller hier ausgeschriebenen Leistungen proaktiv Weiterentwicklungspotenziale aufzuzeigen, die zur Zielerreichung und damit zur Stärkung der Wettbewerbsposition der SBK beitragen.

1.2 Inhalt des Vergabeverfahrens / Auftragsgegenstand

Gegenstand dieser Vergabe ist ein Rahmenvertrag mit bis zu drei Vertragspartnern über Unterstützungs- und Beratungsleistungen für die Planung, Konzeption, Entwicklung und den Betrieb von Softwareindividuallösungen mit Technologieschwerpunkt Java / JavaScript. Die Leistungen erstrecken sich über alle Phasen des Softwarelebenszyklus *(Anforderungsanalyse, Design / Planung, Entwicklung, Test, Integration / Deployment, Betrieb / Instandhaltung)* und umfassen dabei die Tätigkeitsfelder:

Entwicklung gesamt

- Business Analyst (Senior)
- Business Analyst (Professional)
- IT-Projektmanager (Senior)
- IT-Projektmanager (Professional)
- Software- / Lösungsarchitekt (Senior)
- Java Full Stack Software Entwickler (Senior)
- Java Full Stack Software Entwickler (Professional)
- Java Full Stack Software Entwickler (Junior)
- Platform- / DevOps Engineer (Senior)

Betrieb gesamt

- IT-Betriebsspezialist (Junior)
- IT-Betriebsspezialist (Professional)
- IT-Betriebsspezialist (Senior)
- Regressionstester (Junior)

Zum Zeitpunkt des Vertragsabschlusses kann der Bedarf an Entwicklungs-, Betriebs- und Beratungsleistungen zu und im Kontext von Softwareindividuallösungen, der während der Laufzeit der Rahmenvereinbarung

auftritt, nicht abschließend beschrieben werden. Zumal dieser auch durch sich ändernde Rahmenbedingungen (u.a. gesetzliche Anforderungen) einem fortschreitenden Wandel unterliegt.

Auf Grundlage der Rahmenvereinbarung kann der Auftraggeber daher Leistungen in Form von Einzelbeauftragungen *(Direktabruf oder Mini-Wettbewerb)* abrufen, die einen konkreten Unterstützungsbedarf aufgreifen. Allein die Einzelbeauftragungen regeln die konkreten Arbeitspakete und beschreiben den Leistungsumfang. Die Leistungsbestandteile für ein Vorhaben können vollumfänglich oder teilweise über eine Einzelbeauftragung abgerufen werden.

Bei der Realisierung der Entwicklungsvorhaben und dem Betrieb der Softwareindividuallösungen arbeiten der Auftragnehmer eng mit den Fachbereichen, dem Projekt- und Produktmanagement, dem IT-Betrieb und der Softwareentwicklung der SBK sowie im Bedarfsfall auch mit anderen Vertragspartnern zusammen.

1.3 Leistungsabgrenzung zu bestehenden IT-Verträgen

- Die Beratungsleistungen zu Entwicklung, Hosting und Betrieb der Digitalen Kundenschnittstelle“ (DKS) sind erstrangig mit dem für diese Leistungserbringung verantwortlichem Dienstleister vertraglich geregelt.
  Im speziellen Bedarfsfall kann nach Abstimmung der SBK mit dem o.g. Dienstleister eine erforderliche Beratungsleistung an einen Rahmenvertragspartner dieses Vertrages beauftragt werden. Die Beauftragung richtet sich nach den Vorgaben dieses Vertrages in der Leistungsbeschreibung
- Die Beratungsleistungen zum „IT Beratung“ *(außerhalb der hier genannten Leistungsgegenstände)* sowie die Umsetzungsunterstützung in der Organisation sind erstrangig mit den für diese Leistungserbringung verantwortlichen Dienstleistern vertraglich geregelt.
  Im speziellen Bedarfsfall kann nach Abstimmung der SBK mit den o.g. Dienstleistern ein Rahmenvertragspartner dieses Vertrages mit einer erforderlichen Leistung beauftragt werden. Die Beauftragung richtet sich nach den Vorgaben der Leistungsbeschreibung dieses Vertrages.
- Die Beratungsleistungen zum „IT-Security-Dienstleistungen“ sowie die Umsetzungsunterstützung in der Organisation sind erstrangig mit den für diese Leistungserbringung verantwortlichen Dienstleistern vertraglich geregelt.
  Im speziellen Bedarfsfall kann nach Abstimmung der SBK mit den o.g. Dienstleistern ein Rahmenvertragspartner dieses Vertrages mit einer erforderlichen Leistung beauftragt werden. Die Beauftragung richtet sich nach den Vorgaben der Leistungsbeschreibung dieses Vertrages.

1.4 Zeitlicher Überblick

Stand November 2026 *(Bekanntmachung Teilnahmewettbewerb)* ist folgende zeitliche Planung vorgesehen:

Aktivität / Meilenstein	Voraussichtliche Termine
Aufforderung der Bieter zur Angebotsabgabe	Ende Januar 2027
Verhandlungsrunden	März/ April 2027
Zuschlag	Mai 2027
Vertragsbeginn	Juni 2027
Kickoff	Zu Vertragsbeginn

Tabelle 1: Zeitlicher Überblick

1.5 Auftragsvolumen

Aufgrund der anstehenden Entwicklungsprojekte und mit Blick auf die Vergangenheit beläuft sich das geschätzte jährliche Auftragsvolumen auf durchschnittlich 500 Personentage/Jahr.

Das tatsächliche Auftragsvolumen kann in Abhängigkeit der freigegebenen Projektaufträge davon abweichen.

	Anteil in %	Anzahl PT´s jährlich	Anzahl PT´s 4 Jahre
Entwicklung			
Business Analyst (Senior)	3%	15	60
Business Analyst (Professional)	2%	10	40
IT-Projektmanager (Senior)	1%	5	20
IT-Projektmanager (Professional)	1%	5	20
Software- / Lösungsarchitekt (Senior)	3%	15	60
Java Full Stack Software Entwickler (Senior)	4%	20	80
Java Full Stack Software Entwickler (Professional)	3%	15	60
Java Full Stack Software Entwickler (Junior)	1%	5	20
Platform- / DevOps Engineer (Senior)	2%	10	40
Zwischensumme Entwicklung	20%	100	400
Betrieb			
IT-Betriebsspezialist (Junior)	25%	125	500
IT-Betriebsspezialist (Professional)	10%	50	200
IT-Betriebsspezialist (Senior)	5%	25	100
Regressionstester (Junior)	40%	200	800
Zwischensumme Betrieb	80%	400	1.600
Gesamt	100%	500	2.000

1.6 Ort der Leistungserbringung

SBK Zentrale
Heimeranstr. 31
80339 München

"Ort der Leistungserbringung" im Sinne dieses Verfahrens meint den Ort, an dem der Leistungserfolg (Werkleistungen) bzw. das Leistungsergebnis (Dienstleistungen) eintreten muss; dies schließt nicht aus, dass der Auftragnehmer die Tätigkeiten, die zu diesem Leistungserfolg / Leistungsergebnis führen, an einem anderen Ort als München durchführen kann. In der jeweiligen Einzelbeauftragung wird der Ort der Leistungserbringung *(Vor-Ort oder remote)* explizit festgelegt.

2 Anforderungen aus dem Rahmenvertrag

2.1 SBK-spezifische Informationen

Die IT in der SBK ist in folgende Bereiche aufgeteilt:

- IT Betrieb Applikationen und Infrastruktur (ITB AI)
- IT Betrieb Digitale Kundenprozesse (ITB DK)
- IT Wertschöpfung (IT WS)

Der Fachbereich „Systementwicklung (SE)“ des Bereichs IT WS trägt die technische Gesamtverantwortung auch für die Entwicklungsvorhaben, die über den vorliegenden Rahmenvertrag konzipiert und realisiert werden, und legt somit die entwicklungsbezogenen Anforderungen fest. Demgegenüber liegt die technische Gesamtverantwortung für den Betrieb bei den Fachbereichen „CRM und Applikationen“ und „IT-Infrastruktur“.

In der SBK erfolgt die interdisziplinäre Zusammenarbeit bei Entscheidungsprozessen hauptsächlich über Gremien. Für IT Vorhaben gibt es daher ein Architektur- und Entwicklungsboard, in welchem beispielsweise Architekturkonzepte für Neuentwicklungen oder architektonische Veränderungen von Bestandslösungen vorgestellt und zur Freigabe gebracht werden müssen.

Auch im operativen Change- und Releaseprozess gibt es mit dem Change Advisory Board (CAB) ein Gremium, in welchem Vertreter aller IT-Fachbereiche mögliche Überschneidungen und Querwirkungen der Releases bewerten. Das CAB ist daher über geplante Changes und Releases zu informieren.

2.2 Anforderungen an die Zusammenarbeit

2.2.1 Zentraler Ansprechpartner (Key Account Manager)

Der Auftragnehmer hat der SBK einen zentralen Ansprechpartner mit Zuschlagserteilung namentlich zu benennen. Bei Abwesenheit des Ansprechpartners ist ein Stellvertreter mit vergleichbarem Dienstalter (z.B. Ersatz „Senior-Level“-Mitarbeiter durch „Senior-Level“-Mitarbeiter) und genereller Erfahrung mit dem Ausschreibungsgegenstand zu benennen. Der Stellvertreter muss in der Lage sein, die Aufgaben des zentralen Ansprechpartners nach einer angemessenen, im Regelfall kurzen Einarbeitung ohne wesentliche Qualitätseinbußen übernehmen zu können. Sowohl der zentrale Ansprechpartner als auch (im Einzelfall) dessen Stellvertreter müssen in Vollzeit beschäftigt sein, um die Verfügbarkeit nach Ziffer 2.2.2 gewährleisten zu können.

Der zentrale Ansprechpartner bzw. dessen Stellvertreter muss mindestens zu folgenden Themen Auskunft geben und Klärungen herbeiführen können:

- Überblick und Status der Einzelbeauftragungen / Projekte, inkl. proaktiver Meldung von Ressourcenengpässen, Priorisierungsbedarfen sowie Abweichungen von vereinbarten Rahmenbedingungen (z. B. Projektverzögerungen)
- Kaufmännische Fragestellungen
- Optimierung der bestehenden Prozesse zu Produkten / Lösungen, Dienstleistungen, Services und Zusammenarbeit
- Qualitätssicherungsmaßnahmen bezogen auf den Vertragsgegenstand (z.B. bzgl. der Qualität der angebotenen Profile)
- Grundlegende Beratung des Auftraggebers im Rahmen der laufenden Vertragsdurchführung

Der zentrale Ansprechpartner ist die zentrale Kommunikationsinstanz des Auftragnehmers. Die regelmäßige Zusammenarbeit des zentralen Ansprechpartners findet vorrangig mit dem Dienstleistersteuerer der SBK und dessen Vertretung statt.

Hiervon abgegrenzt sind regelmäßige Abstimmungen zwischen den jeweiligen Projektbeteiligten auf Seiten des Auftragnehmers und des Auftraggebers.

Der Dienstleistersteuerer der SBK kommuniziert die Namen der Projektverantwortlichen schriftlich an den Auftragnehmer.

Die erwartete Verfügbarkeit des zentralen Ansprechpartners ist in Ziffer 2.2.2 festgelegt.

2.2.2 Verfügbarkeit zentraler Ansprechpartner

Der zentrale Ansprechpartner oder dessen qualifizierte Vertretung müssen der SBK für Abstimmungen und Absprachen von Montag bis Freitag, außer an gesetzlichen bzw. regional relevanten Feiertagen, innerhalb von 8 Stunden innerhalb der arbeitsvertraglich üblichen Arbeitszeit eines in Vollzeit beschäftigten Mitarbeiters, sowohl telefonisch zum ortsüblichen Festnetztarif oder unter einer kostenfreien Rufnummer und per E-Mail zur Verfügung stehen.

2.2.3 Auftrags- und Vertragssprache

Auftrags- und Vertragssprache ist Deutsch. Das Angebot ist in deutscher Sprache auszufertigen. Der Vertrag und die Leistungen sind in deutscher Sprache zu leisten / abzuwickeln. Die Kommunikation zwischen Auftraggeber und –nehmer erfolgt ausschließlich in deutscher Sprache – ausgenommen sind etablierte englische Fachbegriffe. Dies bedingt, dass die Schlüsselfunktionen in Projekten – insbesondere die Senior-Rollen – zwingend mit deutschsprachigen Mitarbeitenden an deutschen Standorten zu besetzen sind. Die Mindestanforderung liegt bei C1 des CEFRL. So ist sichergestellt, dass zu jeder Zeit und zu allen Fachthemen ein qualitativer Austausch möglich ist. Für das gesamte Projektteam gehen wir von einer Onsite-Quote in Deutschland von mind. 80% aus. In den jeweiligen Einzelbeauftragungen können abweichende Vereinbarungen getroffen werden.

2.2.4 Nearshoring im Europäischen Wirtschaftsraum (EWR)

Die Verlegung betrieblicher Aktivitäten ins nahegelegene Ausland — hier: innerhalb des Europäischen Wirtschaftsraums (EWR), bietet die Möglichkeit, während der Leistungserbringung zusätzliche Personalkapazitäten zu generieren und gleichzeitig Wirtschaftlichkeitspotenziale zu heben. Aufgrund datenschutzrechtlicher Vorgaben ist Nearshoring im Kontext einer künftigen Rahmenvereinbarung nur innerhalb des Europäischen Wirtschaftsraums (EWR) möglich.

Nearshoring ist ferner nur dann zulässig, wenn die Anforderungen zu den Entwicklungsleistungen aus der Leistungsbeschreibung im vorliegenden Dokument sowie zur Zusammenarbeit in der kommenden Leistungsbeschreibung eingehalten werden. Alle zusätzlichen organisatorisch-technischen Maßnahmen, wie zum Beispiel zusätzliche Qualitätssicherung, die durch ein Nearshoring entstehen, gehen zu Lasten des Auftragnehmers.

Zusätzlich ist sicherzustellen, dass Nearshore-Entwickler über Deutsch als Muttersprache oder Deutschkenntnisse auf dem Niveau C1 gemäß dem „Gemeinsamen Europäischen Referenzrahmen für Sprachen" (oder eine vergleichbare Qualifikation) verfügen. Für den Fall, dass in einem Projektverlauf englischsprachige Skillprofile benötigt werden, können alternativ auch englischsprachige Nearshore-Ressourcen angefordert werden.

2.2.5 Leitplanken der Zusammenarbeit

Bei der Zusammenarbeit sind stets folgende Leitplanken zu beachten:

- Ausgeprägtes Produktivitäts- und Qualitätsverständnis: Jedes Umsetzungsvorhaben generiert unmittelbar Wertschöpfungs- und strategische Potenziale für die SBK und ihre Kunden. Der Auftragnehmer erbringt daher zu jederzeit eine qualitativ hochwertige Dienstleistung und wirkt zugleich darauf hin, die Time-to-Market und die Kosten möglichst zu reduzieren.
- Exzellente Nutzerzentrierung: Die Bedarfe unserer Nutzer (hier: Endkunden, interne Anwender bzw. das Entwicklungs- oder Betriebsteam der SBK) werden bei der Entwicklung und dem Betrieb von Softwareindividuallösungen konsequent in den Mittelpunkt gestellt. Ziel ist es, ein möglichst gewinnbringendes und nachhaltiges Nutzererlebnis zu erzielen.
- Proaktive, transparente Kommunikation: Die vertrauensvolle Zusammenarbeit setzt ein hohes Maß proaktiver Kommunikation voraus. Die SBK erwartet deshalb vom Auftragnehmer über veränderte Rahmenbedingungen proaktiv und frühzeitig informiert zu werden, beispielsweise bei Verzögerungen / Komplikationen in Projekten. Auch der Auftraggeber geht mit Fragen oder bei Bekanntwerden von Problemen proaktiv auf den Auftragnehmer zu.
- Agile Produktentwicklung: Die Produktentwicklung erfolgt grundsätzlich nach einem agilen Vorgehensmodell, bei der der Auftraggeber als Product Owner agiert.
- Agile Produktentwicklung ist nicht gleichzusetzen mit agilem Projektmanagement: Die SBK nutzt im Zuge des Projektmanagements überwiegend nicht-iterative Vorgehensmodelle. Aus diesem Grund muss der Auftragnehmer auch in der Lage sein, Projekte in linearer, nicht iterativer Arbeitsweise auf Basis eines Lasten- und Pflichtenhefts mit verbindlich einzuhaltendem Festpreis und Fertigstellungstermin umzusetzen. In diesem Vorgehensmodell werden Änderungen über zusätzlich abzurechnende Abrufe beauftragt.

Im Fall von Abweichungen bei vereinbarten Projektparametern, die die Lieferzeit, den Lieferumfang, die Lieferqualität oder den vereinbarten Preis betreffen, informiert der Auftragnehmer proaktiv, spätestens zwei Werktage nach Bekanntwerden schriftlich den Auftraggeber. Auch der Auftraggeber geht mit Fragen oder bei Bekanntwerden von Risiken und Abweichungen proaktiv auf den Auftragnehmer zu – es wird proaktiv und transparent kommuniziert.

Als Eskalationsgremium wird ein Steering Board benannt, das mindestens aus folgenden Personen besteht:

- Führungskraft des Projekt- / Produktverantwortlichen (SBK)
- Projekt- / Produktverantwortlicher (SBK)
- Dienstleistersteuerer (SBK)
- Führungskraft verantwortliche Einheit (Auftragnehmer)
- Zentraler Ansprechpartner (Auftragnehmer)
- ggf. (themenabhängig):
- Weitere Vertreter des internen Entwicklungsteams (SBK)
- Weitere Vertreter des internen Betriebsteams (SBK)
- Fachverantwortliche (SBK)

2.2.6 Qualitätsmanagement

Die SBK wird mit dem Auftragnehmer jährliche Projekt-Reviews durchführen, welche vorzugsweise in den Räumlichkeiten der SBK in München abgehalten werden. Von Seiten des Auftragnehmers hat mindestens der zentrale Ansprechpartner teilzunehmen. Die jeweilige Agenda wird vier Wochen vor dem Termin in beiderseitigem Einvernehmen abgestimmt und es werden ggf. weitere Personen für die Teilnahme definiert.

2.3 Anforderungen an die Bieterunternehmen

2.3.1 Zertifizierungen

Qualität, Informationssicherheit und Nachhaltigkeit sind wesentliche Bestandteile des Qualitätsverständnisses der SBK und bilden die Grundlage für die Zusammenarbeit mit externen Dienstleistern. Die SBK erwartet von ihren Vertragspartnern etablierte und nachvollziehbare Managementsysteme, die eine sichere, zuverlässige und qualitativ hochwertige Leistungserbringung gewährleisten.

2.3.1.1 *Verpflichtende Zertifizierung*

Der Bieter muss über eine gültige Zertifizierung seines Informationssicherheitsmanagementsystems nach **ISO/IEC 27001 oder ISO 27001** auf Basis von IT-Grundschutz verfügen.

2.3.1.2 *Weitere Zertifizierungen*

Folgende Zertifizierungen werden bei der Bewertung zusätzlich berücksichtigt:

- **ISO 9001:** Qualitätsmanagementsystem
- **ISO/IEC 27701**: Datenschutzmanagementsystem

2.3.1.3 *Nachweisführung*

- Die Zertifizierungen müssen von einer hierfür akkreditierten Zertifizierungsstelle ausgestellt worden und zum Zeitpunkt der geforderten Nachweisführung gültig sein.
- Der Geltungsbereich der Zertifizierungen muss, die für die ausgeschriebenen Leistungen relevanten Organisationseinheiten und Prozesse umfassen.

2.3.2 IT-Sicherheit

2.3.2.1 *Allgemeine Sicherheitsanforderungen*

Der Auftragnehmer hat im Rahmen seiner Leistungserbringung angemessene technische und organisatorische Maßnahmen zur Gewährleistung der Informationssicherheit nach dem Stand der Technik umzusetzen.

2.3.2.2 *Berücksichtigung SBK-interner Sicherheitsvorgaben in der Softwareentwicklung*

Der Auftragnehmer muss im Rahmen seiner Leistungserbringung die relevanten SBK-internen Anforderungen zur / zum sicheren Softwareentwicklung und -betrieb berücksichtigen und umsetzen. Die Sicherheitsvorgaben der SBK werden nach der Vertragsunterzeichnung dem Auftraggeber vorgestellt. Je nach Einzelauftrag werden auch spezifische Anforderungen an die Sicherheit definiert.

2.3.2.3 *Anforderungen des BSI IT-Grundschutzes*

Der Auftragnehmer muss die für seine Leistungserbringung relevanten Anforderungen des BSI IT-Grundschutz-Kompendiums in der jeweils maßgeblichen Fassung erfüllen. Hierzu zählen insbesondere folgende Bausteine:

- CON.8: Software-Entwicklung
- CON.10: Entwicklung von Webanwendungen
- APP.7: Entwicklung von Individualsoftware
- APP.3.1: Webanwendungen und Webservices
- OPS.1.1.3: Patch- und Änderungsmanagement
- OPS.1.1.6: Software-Tests und -Freigaben

Die Auflistung ist nicht abschließend. Weitere für den jeweiligen Leistungsumfang relevante Bausteine sind entsprechend zu berücksichtigen. Die Anforderungen gelten jeweils insoweit, wie sie auf die vereinbarten Leistungen und den Verantwortungsbereich des Auftragnehmers anwendbar sind. Eine Abgrenzung

der Anwendbarkeit findet im Rahmen der Einzelbeauftragungen in Abstimmung von Auftragnehmer und Auftraggeber statt. Dabei sind grundsätzlich die Basis- und Standard-Anforderungen der einschlägigen Bausteine zu erfüllen. Anforderungen bei erhöhtem Schutzbedarf sind entsprechend dem festgestellten Schutzbedarf und den vereinbarten Sicherheitsanforderungen umzusetzen.

2.3.2.4 *Berücksichtigung des BSI IT-Grundschutz++*

Der Auftragnehmer verpflichtet sich, neben dem bisherigen IT-Grundschutz auch die Weiterentwicklung des BSI IT-Grundschutzes zum IT-Grundschutz++ zu berücksichtigen. Die vom BSI bereits veröffentlichten Anforderungen des IT-Grundschutz++ sind bei der Planung, Konzeption und Entwicklung zu berücksichtigen. Mit der offiziellen Verabschiedung der neuen Methodik und des zugehörigen Anforderungskatalogs sind die für den jeweiligen Leistungsumfang relevanten Anforderungen verbindlich anzuwenden. Der Auftragnehmer muss sicherstellen, dass seine Entwicklungs- und Sicherheitsprozesse mit den Anforderungen des IT-Grundschutz++ vereinbar sind und eine nachvollziehbare Überführung vom bisherigen IT-Grundschutz ermöglicht wird. Die konkrete Umsetzung neuer oder wesentlich geänderter Anforderungen sowie notwendige Übergangsfristen sind mit der SBK abzustimmen. Abweichungen sind nachvollziehbar zu dokumentieren und bedürfen der Zustimmung der SBK.

2.3.2.5 *Einhaltung der Anforderungen des CRA (Cyber Resilience Act)*

Der Auftragnehmer verpflichtet sich, die Anforderungen des CRA in seiner Leistungserbringung umzusetzen.

2.3.2.6 *Sichere Softwareentwicklung*

Der Auftragnehmer muss die Informationssicherheit über den gesamten Softwareentwicklungs- und Produktlebenszyklus hinweg gewährleisten. Hierbei sind insbesondere die Grundsätze Security by Design und Security by Default anzuwenden. Die Entwicklung muss nach einem dokumentierten und nachvollziehbaren Entwicklungsprozess erfolgen. Dieser muss angemessene Sicherheitsmaßnahmen wie sichere Entwicklungsumgebungen, Code-Reviews, Schwachstellenanalysen sowie Sicherheitsprüfungen vor der Bereitstellung umfassen. Bei der Softwareentwicklung sind anerkannte Sicherheitsstandards und Best Practices des Open Worldwide Application Security Project (OWASP) zu berücksichtigen, insbesondere der OWASP Application Security Verification Standard (ASVS), soweit dieser für die jeweilige Anwendung anwendbar ist.

2.3.2.7 *Business Continuity Management*

Der Auftragnehmer muss über angemessene organisatorische und technische Vorkehrungen verfügen, um die Kontinuität der vertraglich vereinbarten Leistungen auch bei schwerwiegenden Störungen sicherzustellen. Die hierfür erforderlichen Prozesse und Maßnahmen sollen sich an anerkannten Standards wie dem BSI-Standard 200-4 bzw. ISO 22301 orientieren. Auf Anforderung der SBK sind entsprechende Nachweise bereitzustellen.

2.3.2.8 *Sicherheitsprüfungen und Penetrationstests*

Die entwickelten Softwarelösungen müssen auf Anforderung der SBK einer Sicherheitsprüfung, insbesondere einem Penetrationstest, unterzogen werden können. Die Durchführung kann durch entsprechend qualifizierte Sicherheitsprüfer des Auftragnehmers, durch die SBK oder durch beauftragte Dritte erfolgen. Der Auftragnehmer muss die Durchführung angemessen unterstützen und die hierfür erforderlichen Informationen und Zugänge im abgestimmten Umfang bereitstellen. Vom Auftragnehmer veranlasste Penetrationstests müssen durch fachlich qualifizierte Personen durchgeführt werden, die unabhängig von der unmittelbaren Entwicklung der geprüften Software sind. Die Ergebnisse der Sicherheitsprüfungen sind der SBK vollständig und zeitnah zur Verfügung zu stellen. Identifizierte Sicherheitslücken sind hinsichtlich ihres Risikos zu bewerten und innerhalb der vereinbarten Fristen zu beheben. Kritische Sicherheitslücken sind der SBK unverzüglich mitzuteilen.

2.3.2.9 *Schwachstellen- und Sicherheitsvorfallmanagement*

Der Auftragnehmer muss über geeignete Prozesse zur Identifikation, Bewertung und Behandlung von Schwachstellen in den von ihm entwickelten oder betreuten Softwarekomponenten verfügen. Hierzu gehört insbesondere die Berücksichtigung von Sicherheitslücken in eingesetzten Drittanbieterkomponenten und Softwarebibliotheken.

Der Auftraggeber kann die Einhaltung eines von Ihm vorgegebenen Schwachstellenmanagementprozess einfordern, sollte der vom Auftragnehmer vorgeschlagene Prozess als ungeeignet seitens Auftraggeber bewertet werden.

Sicherheitsvorfälle, die Auswirkungen auf die Vertraulichkeit, Integrität oder Verfügbarkeit der für die SBK erbrachten Leistungen haben oder haben können, sind der SBK unverzüglich nach Bekanntwerden zu melden.

2.3.2.10 *Audit- und Nachweisrechte*

Der Auftragnehmer verpflichtet sich, der SBK auf Anforderung die Überprüfung der Einhaltung der vereinbarten Informationssicherheitsanforderungen zu ermöglichen. Hierzu gehört insbesondere die Bereitstellung geeigneter Nachweise und Dokumentationen sowie die Unterstützung von Audits durch die Informationssicherheitsorganisation der SBK oder durch von ihr beauftragte Dritte. Die Durchführung erfolgt unter angemessener Berücksichtigung der betrieblichen Belange des Auftragnehmers sowie berechtigter Vertraulichkeits- und Schutzinteressen.

2.3.3 KRITIS und branchenspezifische Sicherheitsanforderungen

Die SBK ist Betreiberin einer Kritischen Infrastruktur und unterliegt den entsprechenden gesetzlichen und regulatorischen Anforderungen an die Informationssicherheit, insbesondere den §§ 30, 31 und 39 des BSI-Gesetzes sowie § 392 SGB V. Der Auftragnehmer muss sicherstellen, dass die von ihm erbrachten Leistungen die Einhaltung dieser Anforderungen durch die SBK ermöglichen und nicht beeinträchtigen.

2.3.3.1 *Einhaltung des B3S GKV/PV*

Der Auftragnehmer ist verpflichtet, die für seinen Leistungsumfang relevanten Anforderungen des „Branchenspezifischen Sicherheitsstandards für gesetzliche Kranken- und Pflegeversicherer“ (B3S GKV/PV) in der von der SBK verbindlich festgelegten Fassung einzuhalten. Dies gilt insbesondere für die Anforderungen an Lieferanten und Dienstleister, die sichere Softwareentwicklung und sicheren Softwarebetrieb, das Risikomanagement, die Behandlung von Sicherheitsvorfällen sowie die Aufrechterhaltung der vereinbarten Dienstleistungen. Die konkret anwendbaren Anforderungen und die jeweiligen Verantwortlichkeiten werden unter Berücksichtigung des Leistungsumfangs, des Schutzbedarfs und der KRITIS-Relevanz zwischen der SBK und dem Auftragnehmer festgelegt.

2.3.3.2 *Mitwirkungs- und Nachweispflichten*

Der Auftragnehmer verpflichtet sich, die SBK bei der Erfüllung ihrer gesetzlichen und regulatorischen Verpflichtungen angemessen zu unterstützen. Hierzu gehören insbesondere:

- Die Bereitstellung erforderlicher Informationen und Nachweise zur Einhaltung der vereinbarten Sicherheitsanforderungen.
- Die Mitwirkung an Sicherheits- und Risikoanalysen sowie an Audits und regulatorischen Nachweisprüfungen.
- Die unverzügliche Meldung sicherheitsrelevanter Ereignisse und möglicher Sicherheitsvorfälle, die Auswirkungen auf die vereinbarten Leistungen oder die Informationssicherheit der SBK haben können.
- Die Unterstützung bei der Untersuchung und Behandlung von Sicherheitsvorfällen sowie bei der Umsetzung erforderlicher Abhilfemaßnahmen.

- Die Gewährleistung der vereinbarten Anforderungen an Verfügbarkeit, Notfallvorsorge und Wiederherstellung.
- Die Umsetzung der im Verantwortungsbereich des Auftragnehmers erforderlichen Maßnahmen zur Protokollierung und Angriffserkennung.

2.3.3.3 *Einbindung von Unterauftragnehmern*

Der Auftragnehmer muss sicherstellen, dass eingesetzte Unterauftragnehmer, soweit sie an der Erbringung sicherheitsrelevanter Leistungen beteiligt sind, denselben einschlägigen Sicherheitsverpflichtungen unterliegen. Die Verantwortung für die Einhaltung und Überwachung dieser Verpflichtungen verbleibt beim Auftragnehmer.

2.3.3.4 *Änderungen regulatorischer Anforderungen*

Änderungen der einschlägigen gesetzlichen oder regulatorischen Anforderungen sowie Fortschreibungen des B3S GKV/PV sind hinsichtlich ihrer Auswirkungen auf die Leistungserbringung zu bewerten. Erforderliche Anpassungen sind in Abstimmung mit der SBK umzusetzen. Abweichungen von den vereinbarten Sicherheitsanforderungen bedürfen der vorherigen Zustimmung der SBK.

2.3.4 Einsatz von KI-/LLM-gestützten Werkzeugen

Der Einsatz von KI- oder LLM-gestützten Werkzeugen durch den Auftragnehmer ist in allen Phasen der Leistungserbringung, einschließlich Konzeption, Entwicklung, Betrieb, Analyse, Dokumentation und Support, grundsätzlich nur nach vorheriger ausdrücklicher Genehmigung durch die SBK zulässig. Dabei sind die SBK-internen Vorgaben und Richtlinien zu beachten. Dies gilt unabhängig davon, ob die Werkzeuge lokal betrieben, als externe Dienste bereitgestellt oder als integrierte Funktionen bestehender Entwicklungs- und Betriebswerkzeuge verwendet werden.

Für den Einsatz gelten folgende Anforderungen:

2.3.4.1 *Genehmigung und Transparenz*

- Der Auftragnehmer muss den geplanten Einsatz von KI-/LLM-Werkzeugen vorab gegenüber der SBK offenlegen und genehmigen lassen. Hierzu sind insbesondere die eingesetzten Werkzeuge und Modelle, deren Anbieter, die vorgesehenen Anwendungszwecke sowie die zu verarbeitenden Daten und Informationen zu benennen.
- Die Genehmigung ist auf den jeweils vereinbarten Einsatzbereich beschränkt. Wesentliche Änderungen, insbesondere der eingesetzten Werkzeuge, Verarbeitungszwecke oder Datenflüsse, bedürfen einer erneuten Genehmigung durch die SBK.
- Ein nicht genehmigter Einsatz von KI-/LLM-Werkzeugen ist unzulässig.

2.3.4.2 *Datenschutz und Informationssicherheit*

- Sämtliche für den Auftrag relevanten gesetzlichen und regulatorischen Anforderungen, insbesondere des Datenschutzes, Sozialdatenschutzes, IT-Sicherheitsrechts sowie branchenspezifischer Regelwerke, sind einzuhalten.
- Die Verarbeitung und Übermittlung von Informationen durch KI-/LLM-Werkzeuge ist ausschließlich im Rahmen der gesetzlichen, vertraglichen und durch die SBK genehmigten Vorgaben zulässig.
- Der vom Auftraggeber bereitgestellte oder im Rahmen des Auftrags erstellte Quellcode, Architekturinformationen, Dokumentationen sowie sonstige geschützte Informationen dürfen nicht zu Trainings-, Fine-Tuning- oder sonstigen Zwecken der Modellentwicklung oder Modellverbesserung verwendet werden. Dies ist durch geeignete technische und organisatorische Maßnahmen sicherzustellen.
- Eine unzulässige Weitergabe oder Offenlegung von Informationen an Dritte, insbesondere an externe KI-/LLM-Dienste oder deren Unterauftragnehmer, ist auszuschließen.
- Qualität und Sicherheit KI-generierter Ergebnisse

- Sämtliche durch KI-/LLM-Werkzeuge erzeugten Inhalte, insbesondere Quellcode, Konfigurationen, Infrastrukturdefinitionen, Skripte und Dokumentationen, unterliegen denselben Sicherheits-, Qualitäts- und Funktionsanforderungen wie manuell erstellte Arbeitsergebnisse.
- Der Auftragnehmer muss sicherstellen, dass die erzeugten Inhalte keine Rechte Dritter verletzen und die vereinbarten urheber- und lizenzrechtlichen Anforderungen erfüllen.
- KI-generierte Arbeitsergebnisse sind vor ihrer Verwendung durch eine fachlich qualifizierte und verantwortliche Person auf Korrektheit, Funktionalität, Qualität und Informationssicherheit zu überprüfen.
- Die Verantwortung für die Qualität, Sicherheit und vertragsgemäße Leistungserbringung verbleibt vollständig beim Auftragnehmer.

2.3.4.3 *Human-in-the-Loop-Prinzip*

- Beim Einsatz von KI-/LLM-Werkzeugen ist das Human-in-the-Loop-Prinzip sicherzustellen. Dies bedeutet, dass eine fachlich qualifizierte Person die KI-gestützten Prozesse angemessen überwacht, deren Ergebnisse überprüft und die Verantwortung für daraus resultierende Entscheidungen und Handlungen übernimmt.
- KI-generierte Ergebnisse dürfen nicht ungeprüft in produktive Systeme, Anwendungen oder betriebliche Prozesse übernommen werden.
- Sicherheitsrelevante Entscheidungen sowie Änderungen an produktiven Systemen dürfen nicht eigenständig durch KI-/LLM-Werkzeuge getroffen oder durchgeführt werden. Hierfür sind stets eine bewusste Prüfung und Freigabe durch eine autorisierte Person erforderlich.
- Der Auftragnehmer muss sicherstellen, dass KI-gestützte Prozesse durch verantwortliche Personen kontrolliert, unterbrochen und bei Bedarf beendet werden können.
- Automatisierter und autonomer KI-Einsatz
- Der Einsatz von KI-/LLM-Werkzeugen erfolgt grundsätzlich manuell und unter unmittelbarer menschlicher Kontrolle.
- Eine automatisierte Nutzung, insbesondere die Integration in Build-, Test-, Deployment-, Analyse- oder Betriebsprozesse, beispielsweise CI/CD-Pipelines, Monitoring- oder Ticket-Systeme, ist ausschließlich nach vorheriger gesonderter Genehmigung durch die SBK zulässig.
- Gleiches gilt für den Einsatz autonomer oder agentenbasierter KI-Systeme, die eigenständig Aufgaben ausführen, Entscheidungen treffen oder Aktionen in IT-Systemen veranlassen können.
- Auch bei einer genehmigten Automatisierung müssen angemessene menschliche Kontroll- und Freigabemechanismen entsprechend dem Human-in-the-Loop-Prinzip gewährleistet bleiben.
- Ohne eine entsprechende Genehmigung ist jede Form der automatisierten, kontinuierlichen oder unbeaufsichtigten KI-Nutzung untersagt.

2.4 Anforderungen an Projektrollen und Erfahrungsklassen

Der Auftragnehmer setzt für die Leistungserbringung nur entsprechend qualifiziertes Personal ein. Die Mitarbeitenden des Auftragnehmers werden für eine adäquate Personalplanung und Leistungsabrechnung grundsätzlich einer der folgenden Projektrollen bzw. Mitarbeiterkategorien zugeordnet.

Mit Blick auf das zu erwartende Anforderungsniveau der Einzelbeauftragung sind die bestimmte Projektrollen mit einer adäquaten Erfahrungsklasse (Junior, Professional, Senior) zu besetzen. Zudem ist zu prüfen, ob die etablierten Projektrollen durch Mitarbeiter eines Projektbüros (s.u.) oder Werkstudenten (s.u.) entlastet werden können. So sollen einerseits die qualitativen Anforderungen des Auftrags erfüllt und andererseits Kostenvorteile für den Auftraggeber realisiert werden.

An jede Projektrolle sind mit Blick auf die Qualifikation entsprechende Mindestanforderungen geknüpft. Grundsätzlich besteht bei Einzelbeauftragungen aber auch die Möglichkeit, von den Mindestanforderungen je Projektrolle abzuweichen. Sofern der Auftragnehmer beabsichtigt, Mitarbeitende trotz Nichterfüllung der Mindestanforderungen einer Projektrolle zuzuordnen, so ist dies dem Auftraggeber im Rahmen des Abrufverfahrens darzulegen und zu begründen. Eine Zuordnung zu einer Projektrolle bei Nichterfüllung der Mindestanforderungen ist nur nach Zustimmung des Auftraggebers möglich.

2.4.1 Allgemeine Kenntnisse und Fähigkeiten

- **Sprachliche Kompetenz:** Allgemein Deutsch als Muttersprache oder Deutsch auf Niveaustufe C1 gemäß dem „Gemeinsamen Europäischen Referenzrahmen für Sprachen“ (oder vergleichbare Qualifikation).
- **Ausgeprägtes Produktivitäts- und Qualitätsverständnis:** Jedes Umsetzungsvorhaben generiert unmittelbar Wertschöpfungs- und strategische Potenziale für die SBK und ihre Kunden. Der Auftragnehmer erbringt daher zu jederzeit eine qualitativ hochwertige Dienstleistung und wirkt zugleich darauf hin, die Time-to-Market und die Kosten möglichst zu reduzieren.
- **Exzellente Nutzerzentrierung:** Die Bedarfe unserer Nutzer (hier: Endkunden, interne Anwender bzw. das Entwicklungs- oder Betriebsteam der SBK) werden bei der Entwicklung und dem Betrieb von Softwareindividuallösungen konsequent in den Mittelpunkt gestellt. Ziel ist es, ein möglichst gewinnbringendes und nachhaltiges Nutzererlebnis zu erzielen.
- **Proaktive, transparente Kommunikation:** Die vertrauensvolle Zusammenarbeit setzt ein hohes Maß proaktiver Kommunikation voraus. Die SBK erwartet deshalb vom Auftragnehmer über veränderte Rahmenbedingungen proaktiv und frühzeitig informiert zu werden, beispielsweise bei Verzögerungen / Komplikationen in Projekten. Auch der Auftraggeber geht mit Fragen oder bei Bekanntwerden von Problemen proaktiv auf den Auftragnehmer zu.

Zusätzlich je nach Auftragsschwerpunkt

- **Agile Produktentwicklung**: Die Produktentwicklung erfolgt grundsätzlich nach einem agilen Vorgehensmodell, bei der der Auftraggeber als Product Owner agiert.
- **Agile Produktentwicklung ist nicht gleichzusetzen mit agilem Projektmanagement: Die** SBK nutzt im Zuge des Projektmanagements überwiegend nicht-iterative Vorgehensmodelle. Aus diesem Grund muss der Auftragnehmer auch in der Lage sein, Projekte in linearer, nicht iterativer Arbeitsweise auf Basis eines Lasten- und Pflichtenhefts mit verbindlich einzuhaltendem Festpreis und Fertigstellungstermin umzusetzen. In diesem Vorgehensmodell werden Änderungen über zusätzlich abzurechnende Abrufe beauftragt.
- **.NET Entwicklung:** Es kann zu Einzelbeauftragungen kommen, in dem wir einen .NET-Entwickler benötigen (siehe Technologie-Stack)

- Es gelten die vereinbarten Abruf- und Bereitstellungsfristen sowie die geforderte Qualifikationsgüte analog der Rolle Java Full Stack Developer (Senior) bzw. Java Full Stack Developer (Professional)

2.4.2 Business Analyst (Senior)

- Studium der Informatik / Wirtschaftsinformatik / o.ä. oder Ausbildung zum Fachinformatiker mit fachspezifischer Zusatzqualifikation oder vergleichbare Qualifikation
- Mind. 5 Jahre Berufserfahrung in den Bereichen Business Analyse und Requirements Engineering
- Sehr gute Kenntnisse in der Analyse IT-gestützter Geschäftsprozesse, Anforderungsdefinition und -dokumentation sowie in der Geschäftsprozess- und Softwaresystemmodellierung (BPMN 2.0, UML)
- Hervorragende Kommunikations-, Präsentations- und Moderationsfähigkeiten
- Zertifizierung: Certified Professional for Requirements Engineering (CPRE / IREB) oder ähnlich;
- Wünschenswert: Information Technology Infrastructure Library (ITIL)

2.4.3 Business Analyst (Professional)

- Studium der Informatik / Wirtschaftsinformatik / o.ä. oder Ausbildung zum Fachinformatiker mit fachspezifischer Zusatzqualifikation oder vergleichbare Qualifikation
- Mind. 3 Jahre Berufserfahrung in den Bereichen Business Analyse und Requirements Engineering
- Gute Kenntnisse in der Analyse IT-gestützter Geschäftsprozesse, Anforderungsdefinition und -dokumentation sowie in der Geschäftsprozess- und Softwaresystemmodellierung (BPMN 2.0, UML)
- Ausgeprägte Kommunikations-, Präsentations- und Moderationsfähigkeiten
- Zertifizierung: Certified Professional for Requirements Engineering (CPRE / IREB) oder ähnlich

2.4.4 IT-Projektmanager (Senior)

- Studium der Informatik / Wirtschaftsinformatik / o.ä. oder Ausbildung zum Fachinformatiker mit fachspezifischer Zusatzqualifikation oder vergleichbare Qualifikation
- Mind. 7 Jahre Berufserfahrung in der Leitung komplexer (IT-)Projekte mit klassischen und agilen Methoden
- Beherrschen der gängigen Projektmanagement-Instrumente und agiler Methoden
- Hervorragende Kommunikations-, Präsentations- und Moderationsfähigkeiten
- Zertifizierung: Prince2, Project Management Institute (PMI), International Project Management Association (IPMA) Level B / A, Information Technology Infrastructure Library (ITIL), Agile (PSM II, PSO II, PAL, SPS, PSU), Scaled Agile Framework (SAFe) oder ähnlich

2.4.5 IT-Projektmanager (Professional)

- Studium der Informatik / Wirtschaftsinformatik / o.ä. oder Ausbildung zum Fachinformatiker mit fachspezifischer Zusatzqualifikation oder vergleichbare Qualifikation
- Mind. 3 Jahre Berufserfahrung in der Leitung komplexer (IT-)Projekte mit klassischen und agilen Methoden Leistungsbeschreibung zu Softwareindividuallösungen (Schwerpunkt Java / JavaScript)“
- Beherrschen der gängigen Projektmanagement-Instrumente und agiler Methoden
- Hervorragende Kommunikations-, Präsentations- und Moderationsfähigkeiten
- Zertifizierung: Prince2, Project Management Institute (PMI), International Project Management Association (IPMA) Level B / A, Information Technology Infrastructure Library (ITIL), Agile (PSM I, PSO I), Scaled Agile Framework (SAFe) oder ähnlich

2.4.6 Software- / Lösungsarchitekt (Senior)

- Studium der Informatik / Wirtschaftsinformatik / o.ä. oder Ausbildung zum Fachinformatiker für Anwendungsentwicklung oder vergleichbare Qualifikation
- Mind. 7 Jahre Berufserfahrung im Softwareentwicklungs- und Architekturumfeld
- Sehr gute Kenntnisse zu Lösungsarchitekturen nach modernen Architekturprinzipien
- Mehrjährige Erfahrung in der Konzeption und Implementierung zukunftsfähiger Softwarearchitekturen
- Zertifizierung: Certified Professional for Software Architecture (CPSA / iSAQB) oder ähnlich

2.4.7 Java Full Stack Software Entwickler (Senior)

- Ausbildung: Studium der (Wirtschafts-)Informatik oder eine Ausbildung zum Fachinformatiker für Anwendungsentwicklung oder vergleichbare Qualifikation
- Mind. 5 Jahre Berufserfahrung, sehr gute Kenntnisse im Java-Umfeld und in der agilen Entwicklung, schwerpunktsmäßig mit folgendem Tech-Stack: Java (SE v. 21/25), Spring Boot, React, TypeScript, relationale Datenbanken und Microservice-Architekturen
- Process Engineering: Praktische Erfahrung in BPMN 2.0 und Workflow-Engines wie Camunda BPM
- DevOps-Mindset: Souveräner Einsatz von Git, CI/CD-Pipelines sowie Fokus auf Clean Code und TDD

2.4.8 Java Full Stack Software Entwickler (Professional)

- Ausbildung: Studium der (Wirtschafts-)Informatik oder eine Ausbildung zum Fachinformatiker für Anwendungsentwicklung oder vergleichbare Qualifikation
- Mind. 3 Jahre Berufserfahrung, gute Kenntnisse im Java-Umfeld und in der agilen Entwicklung, schwerpunktsmäßig mit folgendem Tech-Stack: Java (SE v. 21/25), Spring Boot, React, TypeScript, relationale Datenbanken und Microservice-Architekturen
- Process Engineering: Praktische Erfahrung in BPMN 2.0 und Workflow-Engines wie Camunda BPM
- DevOps-Mindset: Souveräner Einsatz von Git, CI/CD-Pipelines sowie Fokus auf Clean Code und TDD

2.4.9 Java Full Stack Software Entwickler (Junior)

- Ausbildung: Studium der (Wirtschafts-)Informatik oder eine Ausbildung zum Fachinformatiker für Anwendungsentwicklung oder vergleichbare Qualifikation
- Gute Kenntnisse im Java-Umfeld und in der agilen Entwicklung, schwerpunktsmäßig mit folgendem Tech-Stack: Java (SE v. 21/25), Spring Boot, React, TypeScript, relationale Datenbanken und Microservice-Architekturen
- DevOps-Mindset: Souveräner Einsatz von Git, CI/CD-Pipelines

2.4.10 Platform- / DevOps Engineer (Senior)

- Ausbildung: Studium der (Wirtschafts-)Informatik oder Ausbildung zum Fachinformatiker oder vergleichbare Qualifikation
- Berufserfahrung: Mindestens 5 Jahre Erfahrung als Platform Engineer, DevOps Engineer oder in vergleichbarer Rolle
- Development & CI/CD: Solide Programmierkenntnisse in Java/Spring Boot sowie fundierte Erfahrung mit Jenkins, GitLab CI, GitHub Actions oder vergleichbaren Tools
- Cloud & Container: Erfahrung mit Docker, Kubernetes und Cloud-Plattformen; idealerweise auch mit EU-souveränen Cloud-Lösungen
- Infrastructure as Code: Fundierte Kenntnisse in Terraform, Ansible oder vergleichbaren IaC-Tools
- Observability & Security: Erfahrung mit Monitoring-/Observability-Tools (z. B. Prometheus, Grafana, ELK-Stack) sowie Verständnis für Netzwerk-, Sicherheits- und Betriebsthemen

- Platform Mindset: Ganzheitliches Denken, ausgeprägtes Ownership und der Anspruch, durch Automatisierung die Developer Experience und Produktivität im Team zu fördern.

2.4.11 IT-Betriebsspezialist (Senior)

- Ausbildung: Studium der (Wirtschafts-)Informatik oder eine Ausbildung zum Fachinformatiker für Systemintegration oder vergleichbare Qualifikation
- Mind. 5 Jahre Berufserfahrung, sehr gute Kenntnisse in der Durchführung des Incident-, Release- und Changemanagements betreuter IT-Infrastruktursysteme und Plattformen
- Analyse und Bearbeitung (2nd Level) komplexer Supportanfragen inkl. systematischer Dokumentation im Ticket-Tool sowie Übernahme einer Eskalationsfunktion
- ITIL & Dienstleistersteuerung: Sichere, eigenverantwortliche Steuerung von Dienstleistern nach ITIL-Framework (Change-, Incident-, Releasemanagement), inkl. SLA-Verantwortung
- Fundiertes Know-how in der Administration und Weiterentwicklung betreuter IT-Systeme, Applikationen und -Plattformen
- Hohe Eigeninitiative bei der Einarbeitung in neue Systeme und Technologien

2.4.12 IT-Betriebsspezialist (Professional)

- Ausbildung: Studium der (Wirtschafts-)Informatik oder eine Ausbildung zum Fachinformatiker für Systemintegration oder vergleichbare Qualifikation
- Mind. 3 Jahre Berufserfahrung, gute Kenntnisse in der Durchführung des Incident-, Release- und Changemanagements betreuter IT-Infrastruktursysteme und Plattformen
- Analyse und Bearbeitung (1st & 2nd Level) von Supportanfragen inkl. systematischer Dokumentation im Ticket-Tool
- ITIL & Dienstleistersteuerung: Erfahrung in der Steuerung von Dienstleistern nach ITIL-Framework (Change-, Incident-, Releasemanagement)
- Gute Kenntnisse in der Administration betreuter IT-Systeme, Applikationen und -Plattformen
- Große Bereitschaft zur Einarbeitung in neue Systeme und Technologien

2.4.13 IT-Betriebsspezialist (Junior)

- Ausbildung: Ausbildung zum Fachinformatiker für Systemintegration oder vergleichbare Qualifikation
- Erste Erfahrungen in der Erfassung, Analyse und Bearbeitung (1st Level) von Supportanfragen sowie in der Dokumentation von Incidents im Ticket-Tool
- ITIL-Grundverständnis: Erste Berührungspunkte mit dem ITIL-Framework (Change-, Incident-, Releasemanagement)
- Grundkenntnisse in der Administration von IT-Systemen, Applikationen und -Plattformen
- Große Bereitschaft zur Einarbeitung in neue Systeme, Tools und Technologien

2.4.14 Regressionstester (Junior)

- Mind. 3 Jahre praktische Erfahrung im Softwaretesten, insbesondere im Bereich Regressionstests
- Fundierte Kenntnisse gängiger Softwaretestmethoden und -verfahren
- Erfahrung in der Erstellung, Durchführung und Dokumentation von Testfällen und Testszenarien
- Sicherer Umgang mit Fehler- und Testmanagementsystemen sowie in der Analyse und Bewertung von Testergebnissen
- Erfahrung mit Softwareentwicklungs- und Releaseprozessen, vorzugsweise in agilen Entwicklungsumgebungen
- Erfahrung im Testen von Schnittstellen und Systemintegrationen
- Zertifizierung nach ISTQB (z. B. Certified Tester Foundation Level oder höher)

- Verständnis für Continuous Integration/Continuous Delivery (CI/CD) und die Einbindung von Tests in Entwicklungs- und Deploymentprozesse
- Grundlegende Kenntnisse in Datenbanken und SQL zur Prüfung und Validierung von Testdaten
  Wünschenswert:
  - Erfahrung mit Testautomatisierung und gängigen Automatisierungswerkzeugen

Ergänzung:

2.5 Leistungsarten und leistungsartspezifische Anforderungen

2.5.1 Business Analyse und Requirements Engineering

Der Auftragnehmer unterstützt die Fachbereiche der SBK mittels moderner und marktüblicher Business Analyse Methoden bei der Identifikation, Analyse, Priorisierung und Formulierung von Fachanforderungen an Prozesse und IT-Systeme. Dabei werden diese unter Berücksichtigung der Geschäftsstrategie der SBK in Lösungskonzepte, die die interne Struktur und die Geschäftsprozesse optimieren, übersetzt. Typische Aufgaben sind u.a. die Analyse und Modellierung von Geschäftsprozessen, die Analyse und Konzeption von Datenmodellen, die Anwendung von Prozessmanagement-Instrumenten sowie die Durchführung von Wirtschaftlichkeits- und Erfolgs- / Risikobetrachtungen. Die Analyseergebnisse sind im Bedarfsfall über die bestehenden Gremien der SBK in adressatengerechter Form vorzustellen.

2.5.2 Projektmanagement und Projektleitung

Der Auftragnehmer kann nach Beauftragung das Projektmanagement bzw. die Projektleitung für Vorhaben zu allen Phasen des Softwarelebenszyklus erbringen. Die Projektsteuerung und –organisation kann dabei sowohl nach agilen als auch klassischen Vorgehensmodellen erfolgen. Notwendige Entscheidungen zur Projektplanung und –durchführung sind im Bedarfsfall über die bestehenden Gremien der SBK in adressatengerechter Form herbeizuführen. Je nach Einzelbeauftragung umfasst diese Leistungsart auch die Koordination und Steuerung weiterer Dienstleister im Auftrag der SBK.

2.5.3 Softwaredesign / -architektur

Bereits bei der Planung und beim Design von Softwareindividuallösungen sind die Bedarfe unserer Nutzer *(hier: Endkunden, interne Anwender bzw. das Entwicklungs- oder Betriebsteam der SBK)* konsequent in den Mittelpunkt zu stellen. Ziel ist es, ein möglichst gewinnbringendes und nachhaltiges Nutzererlebnis zu erzielen. Darüber hinaus sind bei allen Vorhaben die gängigen und etablierten Architektur-Best-Practices und –prinzipien sowie weitere Konzepte (Security-by-desgin, Barrierefreiheit-by-design, etc.) zu berücksichtigen. Ferner wird ein strukturiertes Vorgehen sowie eine dementsprechende Dokumentation in allen Architekturphasen des Lebenszyklus erwartet. Etwaige Architekturkonzepte für Neuentwicklungen oder architektonische Veränderungen von Bestandslösungen werden grundsätzlich im Architekturboard der SBK vorgestellt und zur Freigabe gebracht.

2.5.4 Softwareentwicklung

Im Zuge von Einzelbeauftragungen werden die Neu- oder Weiterentwicklung von Softwareindividuallösungen an einen Auftragnehmer vergeben. In Abhängigkeit des Projektumfangs und –inhalts kann es sein, dass das Entwicklungsvorhaben durch ein gemischtes Projektteam, bestehend aus Vertretern der internen Softwareentwicklung der SBK und der Rahmenvertragspartner, umgesetzt wird. Die Projektorganisation bzw. –zusammensetzung wird in Abstimmung mit dem Auftragnehmer in der Einzelbeauftragung definiert.

2.5.4.1 *Nachhaltigkeit*

Der Auftragnehmer (AN) hat bei Konzeption, Entwicklung und Weiterentwicklung der Software die Grundsätze einer ressourcen- und energieeffizienten Softwareentwicklung („Green Coding“) zu berücksichtigen. Ziel ist es, die geforderte Funktionalität mit einem angemessenen und möglichst geringen Einsatz von Rechen-, Speicher- und Übertragungsressourcen zu realisieren.

Hierzu sind insbesondere folgende Grundsätze zu berücksichtigen:

- **Ressourceneffiziente Architektur und Implementierung**: Unnötige Rechenoperationen, Hintergrundprozesse, Datenübertragungen und technische Abhängigkeiten sind zu vermeiden. Algorithmen, Datenstrukturen und technische Komponenten sind unter Berücksichtigung des Ressourcenbedarfs angemessen auszuwählen. Dabei ist auch auf eine angemessene Skalierbarkeit der Lösung bei unterschiedlichen Nutzungslasten zu achten.
- **Daten- und Speichereffizienz**: Datenhaltung, Datenbankzugriffe, Logging, Caching und temporäre Daten sind bedarfsgerecht zu gestalten. Unnötige oder redundante Datenhaltung ist zu vermeiden.
- **Begrenzung des Ressourcenbedarfs**: Weiterentwicklungen sollen nicht ohne sachlichen Grund zu einer wesentlichen Erhöhung des Bedarfs an Rechenleistung, Arbeitsspeicher, Speicherplatz oder Datenübertragung führen.
- **Integration in den Entwicklungsprozess**: Ressourceneffizienz ist als nichtfunktionale Qualitätsanforderung bei relevanten Architekturentscheidungen, Code Reviews sowie Performance- und Ressourcentests zu berücksichtigen.

2.5.4.2 *Qualitätsstandards*

Die Regelungen zur Quellcode-Qualität und zur Quellcode-Dokumentation sind in Abstimmung mit dem Auftraggeber festzulegen. An der entwickelten Software inkl. des Quellcodes sind die im Vertrag vorgesehenen Nutzungsrechte einzuräumen. Die entwickelte Software inkl. des Quellcodes soll der SBK jederzeit zugänglich sein.

Der Auftragnehmer muss den Quellcode entsprechend den Clean Code Prinzipien, die empfohlene Praktiken für die Entwicklung von lesbarem und wartbarem Quellcode beinhalten, entwickeln. Das Grundkonzept dieser Prinzipien ist es, dass professionell geschriebener Quellcode leicht lesbar ist und seinen Sinn ohne weitere Zusatzdokumentation erkennen lässt. Um die Lesbarkeit des Quellcodes weiter zu erhöhen, arbeitet der Auftragnehmer auf Basis von gewissen Regeln (Konventionen zur Bezeichnung etc.), die dem Auftraggeber zur Verfügung gestellt wurden.

Diese Konventionen werden durch ein Werkzeug zur statischen Quellcode-Analyse im gesamten Entwicklungszyklus automatisiert geprüft. Der Auftragnehmer verwendet die Industriestandard-Regelwerke/-Tools Sonarlint, SpotBugs oder Checkstyle für die statische Quellcode-Analyse. Die Automatisierung wird über ein entsprechendes Werkzeug durch den Auftragnehmer sichergestellt. Entsprechende Qualitätsrichtlinien die in Form von Quality Gates geprüft werden, werden vom Auftraggeber gestellt. Jedes Inkrement muss alle definierten Quality Gates erfolgreich passieren.

Die definierten Quality Gates müssen neben den allgemeinen Qualitätsanforderungen auch angemessene Sicherheitsprüfungen umfassen. Hierzu zählen insbesondere die statische Sicherheitsanalyse des Quellcodes (SAST), die Überprüfung verwendeter Softwarekomponenten und Abhängigkeiten auf bekannte Schwachstellen (SCA) sowie die automatisierte Erkennung von Zugangsdaten und anderen Geheimnissen im Quellcode (Secret Scanning).

Art und Umfang der Sicherheitsprüfungen richten sich nach den eingesetzten Technologien und dem Schutzbedarf der jeweiligen Softwareindividuallösung. Identifizierte Sicherheitslücken sind risikoorientiert zu bewerten und vor der Produktivsetzung entsprechend den vereinbarten Sicherheitsanforderungen zu behandeln. Eine Produktivsetzung mit offenen kritischen oder hohen Sicherheitslücken bedarf einer dokumentierten Risikobewertung und der ausdrücklichen Freigabe durch die SBK.

Die Anforderungen an das Testmanagement sind in Ziffer 2.5.5 beschrieben

Jedes gelieferte Inkrement hat Kriterien zu entsprechen, die der Auftraggeber in der „Definition of Done“ definiert. Folgende Punkte müssen nach aktuellem Stand erfüllt sein, damit das Inkrement als „Fertig“ angesehen wird:

- Alle Akzeptanzkriterien sind erfüllt

- Unit Tests sind erstellt sofern anwendbar
- Code-Review durchgeführt
- Explorativer Entwicklertest erfolgt
- Deployment auf mind. einer Testumgebung erfolgt
- Fachlicher Abnahmetest erfolgt
- Story ist einem Release zugeordnet
- SBK Change Advisory Board (CAB) wurde zum Release informiert
- Qualitätsstandards sind erfüllt
- Die vereinbarten Sicherheitsprüfungen wurden erfolgreich durchgeführt. Identifizierte Sicherheitslücken wurden entsprechend den festgelegten Sicherheitsanforderungen behandelt und erforderliche Ausnahmefreigaben durch die SBK erteilt.
- Deployment auf Produktivumgebung erfolgt

2.5.4.3 *Technologie-Stack*

Folgender Technologie-Stack (Auszug) ist zum Zeitpunkt des Vertragsbeginns als Standard für die Softwareentwicklung definiert.

Der Auftragnehmer muss daher in der Entwicklung und auch im Betrieb mindestens mit diesem Stack umgehen können:

Scope	Technologiebaustein	Eingesetzte Technologie
Desktop Client Entwicklung	**Backend**	.NET
	Frontend	.NET, Electron
Webservice Entwicklung	**Backend**	Java + Spring Boot + Hibernate, Python
	Frontend	TypeScript / JavaScript + React, Shiny
	Deployments	Docker / Kubernetes
Observability	**Monitoring & Alerting**	Elastic Stack
Sonstige Entwicklung	**Messaging**	RabbitMQ (derzeit)
	Synchrone SST	HTTP / REST
	Deployments	Docker / Kubernetes
	Datenbanken	MSSQL, DB2, PostgreSQL, Qdrant, Exasol
	Workflow Processing	Camunda, Airflow
	Codeanalyse	OWASP Toolstack, SonarQube
	Codeverwaltung	GitLab
	Machine Learning / GenAI	Python, R
	Agentic Coding	OpenCode

Der Standard kann sich im Zeitverlauf ändern. Mögliche Updates, Innovationen oder Weiterentwicklungspotenziale für den Technologie-Stack sind durch den Auftragnehmer frühestmöglich und proaktiv gegenüber der SBK zu adressieren. Entscheidungen zu Technologie-Standards sind im Architekturboard der SBK einzubringen.

2.5.4.4 *Dokumentationsstandard*

Für Softwareindividuallösungen sind folgende Dokumentationen in elektronischer und editierbarer Form zu erstellen, zu pflegen und der SBK zu jederzeit zugänglich zu machen:

1. Architektur
    a. Architekturziele und -entscheidungen
    b. Systemkontextmodell
    c. Komponentenmodell
    d. Operational Model
    e. Datenmodell
2. Entwicklung
    a. Dokumentation aller Serviceklassen / Component Klassen und Klassen mit Business Logik (via Javadoc)
    b. API-Dokumentation nach Open API Standard (via Swagger)
    c. Stories und Tasks im Produktbacklog (via Jira), die der abgestimmten Definition of Ready (DoR) entsprechen
3. Betrieb
    a. Installation / Konfiguration
    b. Regelmäßige Service Requests
    c. Post Mortem Dokumentation nach Incidents
4. Anwenderhandbuch

2.5.4.5 *Open-Source-Software*

Der Auftragnehmer hat sicherzustellen, dass Open-Source-Software / -Technologien, die zur Erbringung der Leistung benötigt werden, bestimmungsgemäß und damit entsprechend der jeweiligen Lizenzbedingungen genutzt wird.

2.5.4.6 *Proprietäre Software*

Die Lizenzierung von kostenpflichtigen Technologien für die Entwicklung und den Betrieb der Softwareindividuallösungen liegt bis zu deren vollständigen Übergabe an die SBK im Verantwortungsbereich des Bieters. Die Finanzierung erfolgt grundsätzlich durch den Bieter. Im Bedarfsfall kann in Abstimmung mit der SBK auch ein anderes Finanzierungsmodell angewandt werden.

2.5.4.7 *BITMARCK Software GmbH Partnervertrag*

Für Einzelbeauftragungen, die die Nutzung von Schnittstellen zu unserem Kernsystem BITMARCK_21c|ng umfassen, ist es ggf. erforderlich, einen kostenpflichtigen Partnervertrag für die Überlassung der Schnittstelleninformationen mit der BITMARCK Software GmbH zu schließen. Sofern der Auftragnehmer noch keinen Partnervertrag mit der BITMARCK Software GmbH geschlossen hat bzw. dieser für die Leistungserbringung im Kontext dieser Rahmenvereinbarung nicht herangezogen werden kann, so übernimmt die SBK die Mehrkosten hierfür.

2.5.5 Testmanagement

Ein umfassendes, zielgerichtetes und nachhaltiges Testmanagement prägt letztlich alle Phasen des Softwarelebenszyklus. Das heißt, dass bereits bei der Softwareentwicklung ein testgetriebener Ansatz verfolgt werden muss. Die Ausgangsbasis bilden damit die Unit-Tests, welche aber zwingend durch weitere

funktionale Tests *(Smoke-, Sanity-, Regressions-, Integrations- und Abnahmetests)* ergänzt werden müssen. Ziel ist es, diese Tests weitestgehend zu automatisieren. Die konkreten Testfälle / -szenarien werden im Zuge der Einzelbeauftragung definiert.

Die fachliche Abnahme des Inkrements erfolgt gegen die Akzeptanzkriterien bzw. Testfälle lt. Testplan. Die Experten des Auftragnehmers stehen bei Rückfragen während der Abnahmeprozedur kurzfristig zur Verfügung. Es wird gemeinsam festgelegt, wie mit Fehlern, die im Zuge der Abnahme identifiziert wurden und nicht unmittelbar behoben werden können, umzugehen ist.

2.5.6 Integration / Deployment / Migration

Entwicklungsleistungen muss der Auftragnehmer ausschließlich auf dem von ihm zu betreibenden Entwicklungssystem erbringen. Die SBK stellt dem Auftragnehmer den Zugang zu den SBK-internen Test- und Produktivserverumgebungen zur Verfügung. Der Auftragnehmer ist für das Deployment auf diesen Umgebungen verantwortlich und muss mehrmals täglich einen vollautomatisierten Deployment-Prozess (Continuous Delivery) ohne Ausfallzeiten abbilden können.

Der Auftragnehmer muss sicherstellen, dass die von ihm betriebenen Entwicklungsumgebungen sowie die eingesetzten Build- und Deployment-Prozesse durch angemessene technische und organisatorische Sicherheitsmaßnahmen geschützt sind. Dies umfasst insbesondere die Absicherung der CI/CD-Pipelines gegen unberechtigte Zugriffe und Manipulationen, die sichere Verwaltung von Zugangsdaten, Tokens und kryptografischen Schlüsseln sowie die Nachvollziehbarkeit sicherheitsrelevanter Änderungen und Deployments.

Der Zugriff auf die Test- und Produktivumgebungen der SBK darf ausschließlich über die von der SBK freigegebenen Zugangswege und mit entsprechend autorisierten Berechtigungen erfolgen. Dabei sind insbesondere die Grundsätze der minimalen Rechtevergabe (Least Privilege), der Funktionstrennung und der Nachvollziehbarkeit privilegierter Zugriffe einzuhalten.

Auf den SBK-internen Testumgebungen werden die funktionalen Tests – u.a. für die fachliche Abnahme des betreffenden Inkrements durchgeführt. Der Auftragnehmer hat zugleich den aktuellen Versions- und Konfigurationsstand der Softwareindividuallösung für funktionale Tests anderer Systeme bereitzustellen, sofern dies für diese Tests erforderlich ist.

Der Auftragnehmer muss die Grundsätze eines ordentlichen Change- und Release-Managements, z.B. ITIL, beachten. Über die geplanten Changes und Releases auf der Produktivumgebung ist zudem das SBK Change Advisory Board (CAB) proaktiv zu informieren. Im CAB bewerten Vertreter aller IT-Fachbereiche mögliche Überschneidungen und Querwirkungen der Releases.

Die Bereitstellung von Software und Änderungen in Produktivumgebungen darf ausschließlich nach Abschluss der erforderlichen Qualitäts- und Sicherheitsprüfungen sowie nach erfolgter Freigabe gemäß den Change- und Releaseprozessen der SBK erfolgen. Automatisierte Deployment-Prozesse müssen die Einhaltung dieser Freigabeanforderungen sicherstellen. Eine Umgehung der festgelegten Sicherheitsprüfungen oder Freigabeprozesse durch automatisierte Bereitstellungsverfahren ist unzulässig.

Bei Einführung einer neuen oder weiterentwickelten Softwareindividuallösung muss der Auftragnehmer ggf. auch eine Migration von Daten aus oder in bestehende Systeme planen und durchführen.

Bei der Migration von Daten muss der Auftragnehmer geeignete Maßnahmen zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit der betroffenen Informationen gewährleisten. Dies umfasst insbesondere eine sichere Datenübertragung, die Beschränkung des Datenzugriffs auf autorisierte Personen und Systeme sowie die nachvollziehbare Durchführung und Überprüfung der Migration.

Temporär erstellte Datenbestände und Kopien sind nach Abschluss der Migration sicher zu löschen, sofern keine gesetzlichen oder vertraglichen Aufbewahrungspflichten entgegenstehen. Der Einsatz

produktiver Daten in Entwicklungs- und Testumgebungen ist nur nach vorheriger Freigabe durch die SBK und unter Einhaltung der festgelegten Sicherheits- und Datenschutzanforderungen zulässig.

2.5.7 Applikationsbetrieb und –support

Sofern der Auftragnehmer über diesen Rahmenvertrag eine Softwareindividuallösung für die SBK entwickelt, ist dies nicht automatisch mit der Betriebsunterstützungsleistung verknüpft. Es ist möglich, dass erforderliche Betriebsunterstützungsleistungen einer solchen Entwicklung teilweise oder vollumfänglich von der SBK selbst oder einem Dritten von der SBK beauftragten Unternehmen durchgeführt / übernommen werden.

Es ist geplant Betriebsleistungen in eigenen Leistungsabrufen zu vergeben. Diese Abrufe können Betriebsleistungen für beliebige Softwarelösungen beinhalten. Der Auftragnehmer muss in der Lage sein, sowohl eine Softwarelösung komplett zu betreiben als auch nur Teile des Betriebs (als Ergänzung zum SBK-Betrieb) zu übernehmen.

Für die Übernahme der Betriebsleistungen ist eine Übergabephase zu planen. In dieser Übergabephase werden die technischen (zum Beispiel SLA-Vereinbarungen) und kaufmännischen Rahmenbedingungen (nach Aufwand oder Festpreis) geklärt.

Im Rahmen der jeweiligen Einzelbeauftragung sind die Verantwortlichkeiten für die Informationssicherheit zwischen der SBK, dem Auftragnehmer und gegebenenfalls weiteren beteiligten Dienstleistern eindeutig festzulegen und zu dokumentieren.

Dies umfasst insbesondere die Zuständigkeiten für das Berechtigungsmanagement, Schwachstellen- und Patchmanagement, die Protokollierung und Sicherheitsüberwachung, die Behandlung von Sicherheitsvorfällen sowie die Datensicherung und Wiederherstellung.

Der Auftragnehmer muss sicherstellen, dass die ihm zugewiesenen Sicherheitsaufgaben entsprechend den vereinbarten Anforderungen wahrgenommen werden. Unklare Zuständigkeiten oder erkennbare Sicherheitslücken an den Schnittstellen zu anderen Verantwortlichen sind der SBK unverzüglich mitzuteilen.

Zur Erbringung der Leistung gelten folgende Rahmenbedingungen:

1. Erbringung aller Betriebsleistungen nach den Grundsätzen eines modernen IT-Service-Managements (z.B. Agile Service Management, Lean-IT, ITIL) und Dokumentation in einem Supportkonzept.
2. Kostenfreie Supportnummer oder eine deutsche Rufnummer zum Ortstarif
3. Fehlerhandling / Tracking des SLA via Ticketsystem; (Rück-)Kopplung an das Ticketsystem der SBK muss möglich sein
4. Standard-Supportzeiten Montag bis Freitag 7-18 Uhr außer an bundesweiten Feiertagen und von 8-16 Uhr bei bundesweit nicht einheitlichen Feiertagen
5. Grundsätzlich muss der Auftragnehmer bei entsprechender Notwendigkeit in Absprache mit der SBK (z.B. bei Wartungswochenenden, Release- & Patchdays etc.) den Support auch 24h und an 7 Tagen die Woche (also auch nachts, an Wochenenden und Feiertagen) erbringen. Erfahrungsgemäß handelt es sich hierbei um fünf bis acht Fälle pro Jahr. Davon entfallen üblicherweise vier bis fünf Einsätze auf die Wartungswochenenden unseres Rechenzentrums bei der BITMARCK. Hinzukommen ungeplante Einsätze, die jedoch eine Ausnahme darstellen. Der Auftragnehmer kann für den 24/7-Support einen Preisaufschlag festlegen.
6. Bei Produktübergaben: Schulung von SBK-Mitarbeitern oder Dritten in der Administration und Überwachung. Die Schulung erfolgt als Individualschulung spezifisch nach den Anforderungen und dem Bedarf der SBK. Die Übergabe erfolgt nach einem von der SBK vorgegebenen Standardprozess. Die

Rechte an den hierbei verwendeten oder erstellten Unterlagen gehen vollständig auf die SBK über. Kosten und Aufwände die durch Verzögerungen bei Übergaben, die auf Handeln oder Unterlassen des Auftragnehmers zurückzuführen sind, gehen vollständig zu Lasten des Auftragnehmers.
Für die Abrechnung einer Schulung oder Wissenstransfer wird das entsprechend eingesetzte Rollenprofil mit dem vereinbarten Tagessatz anteilig in Rechnung gebracht.

7. Kontinuierliche Recherche nach funktionalen und sicherheitsrelevanten Patches / Upgrades, proaktive Mitteilung sowie deren Einspielung (auf allen Ebenen: System, Systemsoftware, Anwendungssoftware und Anwendungen).
8. Der Auftragnehmer muss im Rahmen seiner vereinbarten Verantwortlichkeiten sicherstellen, dass bekannt gewordene Sicherheitslücken systematisch identifiziert, hinsichtlich ihres Risikos bewertet und innerhalb der mit der SBK vereinbarten Fristen behandelt werden. Kritische Sicherheitslücken sind unverzüglich an die SBK zu melden. Ist eine zeitnahe Behebung nicht möglich, sind geeignete kompensierende Sicherheitsmaßnahmen vorzuschlagen und mit der SBK abzustimmen. Die Akzeptanz verbleibender Sicherheitsrisiken obliegt der SBK.
9. Sicherstellen und Einhaltung der Anforderungen an Datenschutz und Informationssicherheit für den Betrieb und die Betriebsprozesse. Dies umfasst auch das Bereitstellen und Einspielen von Sicherheitsupdates und laufende Sicherheitsüberprüfungen.
10. Erstellung von monatlichen Servicelevel-Reports basierend auf den ITIL-Grundlagen. Die Reports müssen auch die Erfüllung der vereinbarten Reaktionszeiten und Lösungsquoten enthalten.
11. Durchführen von Last- und Performance-Tests, System- und Integrationstests mit einem entsprechenden Reporting.
12. Für den Betrieb ist ein Monitoring mit der SBK zu vereinbaren und aufzusetzen
13. Das vereinbarte Monitoring muss die für die jeweilige Anwendung und den Verantwortungsbereich des Auftragnehmers relevanten sicherheitsrelevanten Ereignisse berücksichtigen. Der Auftragnehmer muss sicherstellen, dass die hierfür erforderlichen Protokollierungs- und Überwachungsfunktionen bereitgestellt und betrieben beziehungsweise an die zuständigen Sicherheitssysteme der SBK oder weiterer beauftragter Dienstleister angebunden werden können.
14. Der Auftragnehmer muss über geeignete Prozesse zur Erkennung, Bewertung, Meldung und Behandlung von Sicherheitsvorfällen verfügen. Sicherheitsvorfälle sowie begründete Verdachtsfälle, die Auswirkungen auf die Informationssicherheit oder die vereinbarten Leistungen der SBK haben können, sind unverzüglich über die vereinbarten Meldewege an die SBK zu kommunizieren. Die erforderliche Mitwirkung bei der Untersuchung, Eindämmung und Behebung von Sicherheitsvorfällen ist sicherzustellen. Meldewege, Erreichbarkeiten und Reaktionszeiten sind entsprechend der Kritikalität der jeweiligen Anwendung im Leistungsabruf festzulegen.
15. Für den Betrieb sind im Einzelabruf die jeweiligen SLA-Bedingungen zu regeln.
16. Die Applikationsinfrastruktur wird bis auf Weiteres über unser Rechenzentrum bei der BITMARCK bereitgestellt.

2.5.8 Beratung zu den Fachgebieten Softwareentwicklung, -architektur und Applikationsbetrieb

Der Auftragnehmer berät den Auftraggeber zu den Fachgebieten Softwareentwicklung, -architektur und Applikationsbetrieb auf Basis von State-of-the-art-Technologien / -Methodiken sowie Markt- bzw. Branchenkenntnissen. Er unterstützt den Auftraggeber auch bei der Konzeption und Umsetzung von internen Vorhaben, die die prozessualen, organisatorischen und technologischen Perspektiven der o.g. Fachgebiete adressieren und so unmittelbar Optimierungs- und Wertschöpfungspotenziale heben. Dies gilt insbesondere auch für die Förderung und Weiterentwicklung der DevOps-Instrumente beim Auftraggeber. Identifiziert der Auftragnehmer im Zuge einer Einzelbeauftragung entsprechende Potenziale, so sind diese proaktiv beim Auftraggeber zu platzieren