Leistungsbeschreibung

Version: 1.2

Datum: 13.11.2026

Vergabenummer: MD-IT KI-RV 2026

Rahmenvertrag zum Einsatz von KI zur Unterstützung der Krankenhausabrechnungsprüfung sowie zu Compliance, KI-Governance und Managementsystemen

Anlage 03.2 — Fachlos 2: Compliance, Informationssicherheit, Penetrationstests und KI-Governance

MD-IT GmbH

Oudenarder Straße 16
13347 Berlin

Inhaltsverzeichnis

Teil I – Rahmen 4

1 Auftraggeber und Bedarfsträger 4

2 Ausgangslage und Zielsetzung 5

2.1 Ausgangslage bei Compliance und KI-Governance 5

3 Aufteilung in Fachlose, anzuwendende Regelwerke und Begriffsbestimmungen 6

3.1 Anzuwendende Regelwerke 6

3.2 Begriffsbestimmungen 7

Teil II – Leistung 9

4 Leistungen des Fachloses 2 9

4.1 Leistungsgegenstand des Fachloses 2 9

4.2 Stufenweiser Aufbau 10

4.3 Leistungspakete 12

4.4 Abgrenzung zu Fachlos 1 14

4.5 Anforderungen an den Auftragnehmer 15

4.6 Qualifikation des eingesetzten Personals 15

4.7 Projektkoordination 17

4.8 (entfallen) 17

4.9 (entfallen) 17

4.10 Zu übergebende Ergebnisse 17

Teil III – Gemeinsame Bestimmungen 19

5 Geltungsbereich der gemeinsamen Bestimmungen 19

5.1 Geltungsbereich und Schutzbedarf 19

6 Zugänge, Unterlagen und Arbeitsmittel 20

6.1 Identitäts- und Berechtigungsmanagement 20

6.2 Aufbewahrung und Löschung überlassener Unterlagen 20

6.3 Fernzugang 20

7 Protokollierung 21

7.1 Protokollierung und Beweissicherung 21

8 Sichere Arbeitsweise und Vorfälle 21

8.1 Überlassene Test-, Schulungs- und Entwicklungsdaten 21

8.2 Personalsicherheit und Vertraulichkeit 22

8.3 Sichere Entwicklung, Schwachstellen und Lieferkette 23

8.4 Sicherheitsvorfälle 23

9 Prüfrechte und Vertragsende 24

9.1 Prüfrechte, wiederkehrende Überprüfung und Betriebsdokumentation 24

9.2 Datenrückgabe, Löschung und technische Übergabe bei Vertragsende 24

10 Einsatz von Komponenten der künstlichen Intelligenz 25

10.1 Grundsätze für den Einsatz 25

Teil IV – Weitere gemeinsame Bestimmungen 26

11 Gemeinsame Bestimmungen 26

11.1 Verarbeitung von Sozial- und Gesundheitsdaten 26

11.2 Personalsicherheit und Vertraulichkeit 26

11.3 Arbeitsmöglichkeiten und Zugänge 26

11.4 (entfallen) 27

11.5 Abgrenzung zur Rechtsberatung 27

Teil I – Rahmen

1 Auftraggeber und Bedarfsträger

Auftraggeberin der Rahmenvereinbarung ist die MD-IT GmbH. Die nachfolgend aufgeführten Organisationen sind abrufberechtigte Bedarfsträger und können im eigenen Namen Einzelaufträge aus der Rahmenvereinbarung abrufen.

Die Leistungen dieses Fachloses werden vorrangig bei der MD-IT GmbH für den Aufbau und den Betrieb des gemeinschaftlichen Managementsystems erbracht. Daneben kann jeder Bedarfsträger Leistungen für seinen eigenen organisatorischen oder technischen Bedarf abrufen.

Mit jedem Abruf kommt ein eigener Einzelvertrag zwischen dem abrufenden Bedarfsträger und dem Auftragnehmer zustande. Eine Verpflichtung zum Abruf besteht nicht.

Abrufberechtigt sind die nachfolgend genannten Stellen.

Organisation	**Standort und Anschrift**
Medizinischer Dienst Baden-Württemberg	Ahornweg 2, 77933 Lahr
Medizinischer Dienst Bayern	Haidenauplatz 1, 81667 München
Medizinischer Dienst Berlin-Brandenburg	Schlaatzweg 1, 14473 Potsdam
Medizinischer Dienst Bremen	Falkenstraße 9, 28195 Bremen
Medizinischer Dienst Hessen	Zimmersmühlenweg 23, 61440 Oberursel
Medizinischer Dienst Mecklenburg-Vorpommern	Lessingstraße 33, 19059 Schwerin
Medizinischer Dienst Niedersachsen	Hildesheimer Straße 202, 30519 Hannover
Medizinischer Dienst Nord	Hammerbrookstraße 5, 20097 Hamburg
Medizinischer Dienst Nordrhein	Berliner Allee 52, 40212 Düsseldorf
Medizinischer Dienst Rheinland-Pfalz	Albiger Straße 19 d, 55232 Alzey
Medizinischer Dienst Saarland	Dudweiler Landstraße 151, 66123 Saarbrücken
Medizinischer Dienst Sachsen	Am Schießhaus 1, 01067 Dresden
Medizinischer Dienst Sachsen-Anhalt	Breiter Weg 19 c, 39104 Magdeburg
Medizinischer Dienst Thüringen	Richard-Wagner-Straße 2 a, 99423 Weimar
Medizinischer Dienst Westfalen-Lippe	Roddestraße 12, 48153 Münster
Medizinischer Dienst Bund	Theodor-Althoff-Straße 47, 45133 Essen
MD-IT GmbH	Oudenarder Straße 16, 13347 Berlin
Deutsche Rentenversicherung Knappschaft-Bahn-See	Pieperstraße 14–28, 44789 Bochum

Im gesamten Bundesgebiet beschäftigen die Medizinischen Dienste rund 12.000 Mitarbeitende, darunter 2.472 Ärztinnen und Ärzte. Der sozialmedizinische Dienst der Deutschen Rentenversicherung Knappschaft-Bahn-See beschäftigt rund 700 Mitarbeitende in Voll- und Teilzeit.

Die MD-IT – Aufgaben-Überblick

Die MD-IT GmbH ist ein Gemeinschaftsunternehmen der insgesamt 15 Medizinischen Dienste, dem MD Bund und der Deutschen Rentenversicherung Knappschaft-Bahn-See. Die MD-IT wurde mit dem Ziel gegründet, die Zusammenarbeit der Gemeinschaft der Medizinischen Dienste auf dem Gebiet der Informations- und Kommunikationstechnologie weiter zu bündeln.

Zu diesem Zweck wurde ihr die Aufgabe übertragen, eine Branchensoftware auf Basis einheitlicher Geschäftsprozesse zu entwickeln und zu betreiben. Die Branchensoftware, die derzeit unter der Produktbezeichnung MDconnect entwickelt wird, sowie sogenannte Umsysteme sind Bestandteil der Branchenlösung für die Gemeinschaft der Medizinischen Dienste. Als Umsysteme werden Systeme außerhalb der Systemgrenzen der Branchensoftware bezeichnet, die zum Beispiel über Schnittstellen angebunden werden.

2 Ausgangslage und Zielsetzung

Gegenstand dieses Fachloses ist die Unterstützung des Auftraggebers beim Aufbau und Betrieb eines Managementsystems für künstliche Intelligenz sowie bei Compliance, Informationssicherheit, technischen Sicherheitsprüfungen, KI-Governance und Datenschutz für den Einsatz von Anwendungen der künstlichen Intelligenz.

Die Leistung wird als Beratungs- und Unterstützungsleistung erbracht. Ein vom Auftragnehmer betriebener Dienst ist nicht Gegenstand dieses Fachloses.

2.1 Ausgangslage bei Compliance und KI-Governance

Mit dem Einsatz von Systemen der künstlichen Intelligenz entstehen bei den Bedarfsträgern Pflichten, die über die einzelne Anwendung hinausgehen. Die Verordnung (EU) 2024/1689 (KI-Verordnung) verlangt je nach Einordnung des Systems eine dokumentierte Bewertung, eine Risikobeurteilung, die Information der Nutzer und, bei Einstufung als Hochrisiko-KI-System, weitergehende Pflichten des Anbieters und des Betreibers. Hinzu treten die Anforderungen des Sozialdatenschutzes nach den §§ 67 ff. SGB X, der Datenschutz-Grundverordnung und der Informationssicherheit.

Der Auftraggeber baut hierfür ein Managementsystem für den Einsatz von Systemen der künstlichen Intelligenz auf. Es soll die Anforderungen der einschlägigen Regelwerke in prüfbare Vorgaben übersetzen, die für die Anmeldung und den Betrieb von KI-Anwendungen erforderlichen Unterlagen bereitstellen und für weitere Anwendungen wiederverwendbar sein. Es ist damit nicht auf eine einzelne Anwendung beschränkt.

Die Medizinischen Dienste sind rechtlich eigenständige Körperschaften mit eigenen Organisationsstrukturen und teils eigenen Bestandssystemen. Sie setzen künftig eigene KI-Anwendungen ein, deren Art und Umfang derzeit nicht abschließend bekannt sind. Das Managementsystem ist deshalb so auszulegen, dass es von den Medizinischen Diensten, vom Medizinischen Dienst Bund sowie von der Deutschen Rentenversicherung Knappschaft-Bahn-See übernommen oder angebunden werden kann, ohne dass es hierfür neu erstellt werden muss.

Zum Aufbau und zum laufenden Betrieb dieses Managementsystems sowie zu Governance, Compliance, Informationssicherheit und Datenschutz beim Einsatz von KI-Anwendungen wird Unterstützung beschafft. Diese Leistung ist Gegenstand dieses Fachloses.

3 Aufteilung in Fachlose, anzuwendende Regelwerke und Begriffsbestimmungen

Die Leistung wird in drei Fachlose aufgeteilt. Ein Angebot kann auf ein Fachlos, auf mehrere oder auf alle Fachlose abgegeben werden; die Zuschläge erfolgen je Fachlos gesondert. Gegenstand dieser Leistungsbeschreibung ist Fachlos 2.

Für Fachlos 2 wird eine Rahmenvereinbarung geschlossen. Abrufberechtigt sind der Auftraggeber und die übrigen in Kapitel 1 aufgeführten Bedarfsträger. Eine Mindestabnahme besteht nicht; auch die den Stufen 1 und 2 nach Abschnitt 4.2 zugewiesenen Leistungsanteile werden erst mit dem Abruf geschuldet.

Mit jedem Abruf kommt ein eigener Einzelvertrag zwischen der abrufenden Stelle und dem Auftragnehmer zustande; die abrufende Stelle ist Vertragspartnerin und trägt die Vergütung ihres Abrufs.

Ein Mini-Wettbewerb (Wettbewerb um den Einzelauftrag) findet für dieses Fachlos nicht statt; maßgeblich sind die im Vergabeverfahren festgelegten Preise und Tagessätze.

Die Leistungen zum Aufbau des gemeinschaftlichen Managementsystems ruft der Auftraggeber ab; der Höchstwert nach Abschnitt 4.1 gilt kumuliert über sämtliche Abrufe dieses Fachloses.

3.1 Anzuwendende Regelwerke

Der Leistungsbeschreibung liegen die nachstehenden Regelwerke zugrunde, jeweils in der geltenden Fassung. Die Aufzählung benennt die wesentlichen Regelwerke und ist nicht abschließend; weitere Vorschriften bleiben unberührt, soweit sie auf den einzelnen Bedarfsträger oder die konkrete Verarbeitung Anwendung finden.

Rechtlich verbindlich sind, jeweils nach Maßgabe der gesetzlichen Funktion des betreffenden Bedarfsträgers, der Rolle des Auftragnehmers und der konkreten Verarbeitungstätigkeit: für die Verarbeitung personenbezogener Daten und Sozialdaten die Verordnung (EU) 2016/679 (DSGVO), das Bundesdatenschutzgesetz sowie die Datenschutzgesetze der Länder, soweit sie auf den jeweiligen Bedarfsträger Anwendung finden, § 35 des Ersten Buches Sozialgesetzbuch sowie die §§ 67 ff. einschließlich § 67c Absatz 3 und § 80 des Zehnten Buches Sozialgesetzbuch; für Prüfungen, Beratungen und gutachtliche Stellungnahmen der Medizinischen Dienste nach den §§ 275 bis 275c des Fünften Buches Sozialgesetzbuch die Anforderungen des § 276 des Fünften Buches Sozialgesetzbuch; ferner die Verordnung (EU) 2024/1689 (KI-Verordnung) in der durch die Verordnung (EU) 2026/1744 geänderten Fassung, die Verordnung (EU) 2024/2847 (Cyberresilienz-Verordnung) sowie das jeweils auf den Bedarfsträger anwendbare Behindertengleichstellungs- und Barrierefreiheitsrecht des Bundes oder des Landes; unabhängig von dessen unmittelbarer Anwendbarkeit werden die Anforderungen der Barrierefreie-Informationstechnik-Verordnung und der Norm EN 301 549 als einheitliche vertragliche Mindestanforderungen vereinbart. Ergänzend gelten die Vorschriften der Länder zur Informationssicherheit, soweit sie auf den jeweiligen Bedarfsträger Anwendung finden.

Für den Sozialmedizinischen Dienst der Deutschen Rentenversicherung Knappschaft-Bahn-See gelten die §§ 275 bis 277 des Fünften Buches Sozialgesetzbuch nach Maßgabe des § 283a des Fünften Buches Sozialgesetzbuch entsprechend.

Die Deutsche Rentenversicherung Knappschaft-Bahn-See hat mitgeteilt, Pflichten als Betreiberin einer kritischen Anlage zu unterliegen. Soweit dies zutrifft und die im Rahmen dieser Leistungsbeschreibung eingesetzten informationstechnischen Systeme, Komponenten oder Prozesse für die Funktionsfähigkeit dieser kritischen Anlage maßgeblich sind, gelten ergänzend die Vorgaben des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik und der hierzu ergangenen Rechtsverordnung, insbesondere zu Sicherheitsanforderungen, zu Systemen zur Angriffserkennung, zu Meldepflichten und zu den wiederkehrenden Nachweisen. Für die Medizinischen Dienste besteht eine entsprechende Betroffenheit nach derzeitigem Kenntnisstand nicht.

Als technische und organisatorische Maßstäbe herangezogen werden: die Verordnung (EU) 2023/2854 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung, die Normen DIN EN ISO/IEC 27001, DIN EN ISO/IEC 27701 und DIN EN ISO/IEC 42001, die vom Auftraggeber vorgegebenen Sicherheitsanforderungen, die sich aus den Kapiteln 5 bis 10 dieser Leistungsbeschreibung ergeben, die Technischen Richtlinien BSI TR-02102-1 und BSI TR-02102-2, das IT-Grundschutz-Kompendium des Bundesamts für Sicherheit in der Informationstechnik, der Anforderungskatalog Cloud Computing (C5), die Anforderungen des Bundesamts für Soziale Sicherung an cloudbasierte Lösungen in der Sozialversicherung sowie die Normen EN 301 549 und DIN EN ISO 9241.

Jede Bezugnahme auf eine technische Norm, Richtlinie, Zertifizierung oder ein anderes technisches Bezugssystem in dieser Leistungsbeschreibung und ihren Anlagen ist so zu lesen, als sei ihr der Zusatz „oder gleichwertig“ beigefügt; dies gilt für jede einzelne Anforderung, in der eine solche Bezugnahme enthalten ist. Ausgenommen sind Nachweise, die eine zwingende gesetzliche Regelung in bestimmter Form fordert. Die Gleichwertigkeit ist vom Bieter mit geeigneten Mitteln nachzuweisen.

Für dieses Fachlos ergeben sich die Anforderungen aus Kapitel 4 sowie ergänzend aus den nach Kapitel 5 anwendbaren Abschnitten der Kapitel 5 bis 10. Werden die genannten Regelwerke während der Vertragslaufzeit fortgeschrieben, gilt Abschnitt 5.1 Absatz 6.

Die Angaben zu den anwendbaren Regelwerken beschreiben den fachlichen Rahmen der Leistung. Ob und in welchem Umfang eine Vorschrift auf den einzelnen Bedarfsträger Anwendung findet, richtet sich nach dessen gesetzlicher Funktion und ist von diesem eigenständig zu beurteilen.

3.2 Begriffsbestimmungen

Auftraggeber ist die MD-IT GmbH als Auftraggeberin der Rahmenvereinbarung. Sie handelt für dieses Fachlos als zentrale Beschaffungsstelle für die Bedarfsträger und ist zugleich Bedarfsträgerin, soweit sie selbst Leistungen abruft; dies betrifft insbesondere die Leistungen zum Aufbau und Betrieb des gemeinschaftlichen Managementsystems.

Auftragnehmer ist das Unternehmen, das für dieses Fachlos den Zuschlag erhält und mit dem die Rahmenvereinbarung geschlossen wird.

Bedarfsträger sind die in Kapitel 1 aufgeführten abrufberechtigten Organisationen, die Leistungen im eigenen Namen aus der Rahmenvereinbarung abrufen und dadurch Vertragspartner des jeweiligen Einzelvertrags werden.

Abrufende Stelle ist der Auftraggeber oder der Bedarfsträger, der den jeweiligen Einzelvertrag schließt.

Ausgabesicht bezeichnet eine aus einer gemeinsamen Erhebung abgeleitete Darstellung für einen bestimmten Zweck, etwa für eine Datenschutz-Folgenabschätzung oder eine Grundrechte-Folgenabschätzung.

Personentag bezeichnet die Arbeitsleistung einer Person im Umfang der im Preisblatt bestimmten Zahl von Stunden. Die in den Angeboten anzugebenden Tagessätze beziehen sich auf diesen Umfang; gibt ein Bieter einen Stundensatz an, so rechnet er ihn auf dieser Grundlage um. Die Dokumentation des tatsächlichen Aufwands nach der Rahmenvereinbarung (Anlage 26.2) bleibt unberührt.

Teil II – Leistung

4 Leistungen des Fachloses 2

4.1 Leistungsgegenstand des Fachloses 2

Gegenstand des Fachloses 2 ist die Unterstützung des Auftraggebers beim Aufbau und beim Betrieb eines Managementsystems für den Einsatz von Systemen der künstlichen Intelligenz. Daneben umfasst das Fachlos Leistungen, die ein Managementsystem nicht voraussetzen, insbesondere die technischen Sicherheitsprüfungen nach Leistungspaket 6, die Beratungsleistungen nach Leistungspaket 7 und das KI-Red-Teaming nach Leistungspaket 9 des Abschnitts 4.3. Das Managementsystem richtet sich nach der Norm DIN EN ISO/IEC 42001 und ergänzend nach der Norm DIN EN ISO/IEC 27001. Es bildet die Anforderungen der KI-Verordnung sowie die vom Auftraggeber vorgegebenen Sicherheitsanforderungen ab, jeweils in der geltenden Fassung.

Die für alle Fachlose anwendbaren Regelwerke sind in Abschnitt 3.1 aufgeführt.

Sämtliche Leistungspakete werden auf Abruf erbracht; eine Mindestabnahme wird nicht vereinbart. Abrufberechtigt sind der Auftraggeber und die übrigen in Kapitel 1 aufgeführten Bedarfsträger; die abrufende Stelle entscheidet je Leistungspaket über den Abruf. Soweit Leistungen zum Aufbau des gemeinschaftlichen Managementsystems abgerufen werden, erfolgt der Abruf durch den Auftraggeber; daneben kann jeder Bedarfsträger Leistungen für seinen eigenen organisatorischen oder technischen Bedarf abrufen. Die den Stufen 1 und 2 nach Abschnitt 4.2 zugewiesenen Leistungsanteile bilden das für die Aufnahme des Betriebs erforderliche Grundgerüst; sie werden vorrangig abgerufen und sind nach Abruf innerhalb der Fristen des Abschnitts 4.2 zu erbringen. Der Abruf der Stufen 1 und 2 kann zeitgleich mit dem Zuschlag erfolgen; der Auftragnehmer beginnt mit der Leistungserbringung spätestens zwei Wochen nach Abruf.

Für die Leistungen zum gemeinschaftlichen Managementsystem nimmt der Auftraggeber die nachstehenden Mitwirkungspflichten wahr; bei einem eigenen Abruf eines Bedarfsträgers treffen die für den jeweiligen Einzelauftrag erforderlichen Mitwirkungspflichten die abrufende Stelle. Der Auftraggeber benennt für die Leistungen dieses Fachloses Ansprechpersonen und stellt die bei ihm vorhandenen Unterlagen bereit, die für den Aufbau des Managementsystems erforderlich sind, insbesondere zu bestehenden Managementsystemen, zum Risikoregister und zu vorhandenen Mustern. Er gibt Rückmeldungen und trifft Entscheidungen zu vorgelegten Arbeitsergebnissen in der Regel innerhalb von zehn Werktagen. Der Auftraggeber kann einzelne Leistungsanteile selbst erbringen; sie werden im jeweiligen Abruf ausgenommen, und der Auftragnehmer baut auf den übergebenen Ergebnissen auf. Verzögert sich eine Mitwirkung des Auftraggebers, verlängern sich die Fristen nach Abschnitt 4.2 entsprechend; der Auftragnehmer zeigt eine Behinderung unverzüglich in Textform an.

Das Managementsystem wird bei der MD-IT aufgebaut. Es ist so auszulegen, dass es von den Medizinischen Diensten, vom Medizinischen Dienst Bund sowie von der Deutschen Rentenversicherung Knappschaft-Bahn-See übernommen oder angebunden werden kann, ohne dass es hierfür neu erstellt werden muss. Vorzusehen ist eine Struktur aus einem gemeinsamen Kern und daran anschließenden

organisationsbezogenen Teilen; der Auftragnehmer beschreibt, wie diese Struktur ausgestaltet wird und welche Teile gemeinsam und welche je Organisation geführt werden.

Das Managementsystem wird in der für den jeweiligen Abruf von der abrufenden Stelle bereitgestellten oder bezeichneten Umgebung abgebildet; bei den Leistungen zum gemeinschaftlichen Managementsystem ist dies die Umgebung des Auftraggebers. Der Auftragnehmer arbeitet in dieser Umgebung und übergibt Arbeitsergebnisse dort. Künftig soll das Managementsystem in der Lösung des Fachloses 3 geführt werden; der Auftraggeber teilt dem Auftragnehmer den Zeitpunkt des Wechsels mit. Vorlagen, Richtlinien und sonstige Ergebnisse sind deshalb so zu erstellen, dass sie pflegbar und versionierbar sind, in eine andere Umgebung übernommen werden können und ohne Werkzeuge des Auftragnehmers weitergeführt werden können. Ein Anspruch auf Nutzung einer bestimmten Plattform besteht nicht.

Der Grundaufbau des Managementsystems einschließlich der Stufen 1 und 2 nach Abschnitt 4.2 ist nach Maßgabe der Fristen des Abschnitts 4.2 abzuschließen. Die Leistungen der Stufe 3 werden nach Maßgabe des Abschnitts 4.2 gesondert abgerufen. Der Auftragnehmer legt hierfür einen Zeitplan vor, der die Abhängigkeit zur Einführung der Lösung aus Fachlos 1 berücksichtigt.

Der Höchstwert der Rahmenvereinbarung für das Fachlos 2 beträgt 26.000.000 EUR netto einschließlich der Reisekosten nach Abschnitt 11.3 Absatz 2 und etwaiger Preisanpassungen nach der Rahmenvereinbarung (Anlage 26.2); mit seinem Erreichen ist die Rahmenvereinbarung für dieses Fachlos ausgeschöpft. Eine Höchstabrufmenge in Personentagen wird nicht festgelegt. Die im Preisblatt (Anlage 07.2) angegebenen Personentage (insgesamt 20.000 über die Laufzeit) sind Schätz- und Wertungsmengen; sie dienen der Angebotswertung und der Auftragswertschätzung, begrenzen die Abrufe nicht und begründen keinen Anspruch des Auftragnehmers auf einen bestimmten Abrufumfang. Reisezeiten werden nach Abschnitt 11.3 Absatz 2 nicht vergütet.

Die Rahmenvereinbarung hat eine Laufzeit von vier Jahren ab Zuschlag. Vertragsjahr ist jeweils der Zeitraum von zwölf Monaten ab Zuschlag oder dessen Jahrestag. Die Laufzeit der Einzelverträge richtet sich nach der Rahmenvereinbarung.

Das Managementsystem ist so aufzubauen, dass es für weitere KI-Anwendungen des Auftraggebers und der Bedarfsträger wiederverwendbar ist, einschließlich Anwendungen, die als Hochrisiko-KI-Systeme im Sinne der KI-Verordnung einzustufen sind.

4.2 Stufenweiser Aufbau

Das Managementsystem wird in drei aufeinander aufbauenden Stufen errichtet. Der Auftragnehmer legt seiner Planung diese Reihenfolge zugrunde; eine Stufe wird abgeschlossen und von der abrufenden Stelle abgenommen, bevor die nachfolgende begonnen wird; bei den Leistungen zum gemeinschaftlichen Managementsystem ist dies der Auftraggeber. Arbeiten an einer späteren Stufe können vorgezogen werden, soweit sie die Fertigstellung der laufenden Stufe nicht beeinträchtigen.

Stufe 1: Grundgerüst. Geltungsbereich und Politik des Managementsystems, Rollen und Verantwortlichkeiten, Verzeichnis der eingesetzten und geplanten KI-Systeme sowie die zugehörige Dokumentenlenkung. Mit Abschluss dieser Stufe verfügt die abrufende Stelle über eine tragfähige Grundlage, auf

der die weiteren Verfahren aufsetzen; bei den Leistungen zum gemeinschaftlichen Managementsystem ist dies der Auftraggeber.

Stufe 2: Bewertungsverfahren. Aufbau des integrierten Assessments mit einer gemeinsamen Erhebungsschicht und den daraus abgeleiteten Ausgabesichten, insbesondere Datenschutz-Folgenabschätzung nach Art. 35 DSGVO, Grundrechte-Folgenabschätzung nach Art. 27 der KI-Verordnung, soweit für den jeweiligen Einsatz erforderlich, Prüfung nach den Vorschriften über Sozialdaten, Betreiberpflichten nach Art. 26 der KI-Verordnung sowie Anbindung an das Risikoregister der abrufenden Stelle, bei den Leistungen zum gemeinschaftlichen Managementsystem an das Risikoregister des Auftraggebers. Die Erhebungsschicht ist für alle Organisationen einheitlich; die Unterschiede zwischen den Organisationen werden in den Ausgabesichten abgebildet. Die Erhebungsschicht ist so aufzubauen, dass Teile der Datenschutz-Folgenabschätzung nach Art. 35 DSGVO in die Grundrechte-Folgenabschätzung übernommen oder dort in Bezug genommen werden können, soweit sie die dortigen Anforderungen erfüllen.

Stufe 3: Betrieb und Verbesserung. Überwachung und Messung der Wirksamkeit, interne Audits, Managementbewertung, Verfahren zur Verbesserung sowie Lieferantensteuerung und Lebenszyklussteuerung der KI-Systeme von der Einführung bis zur Außerbetriebnahme.

Stufe 1 ist innerhalb von zwölf Wochen nach Abruf abzuschließen; Stufe 2 ist innerhalb weiterer sechzehn Wochen nach Abschluss der Stufe 1, insgesamt also spätestens innerhalb von achtundzwanzig Wochen nach Abruf, abzuschließen. Für die Einhaltung dieser Fristen genügt, dass der Auftragnehmer die Ergebnisse der jeweiligen Stufe vollständig und abnahmefähig vorgelegt hat. Die abnehmende Stelle entscheidet über die Abnahme innerhalb der im Einzelvertrag vereinbarten Prüffrist; ist keine vereinbart, beträgt sie zehn Werktage ab der abnahmefähigen Vorlage. Verzögert sich die Abnahme über diese Frist hinaus aus Gründen, die die abnehmende Stelle zu vertreten hat, so verschieben sich der Beginn der nachfolgenden Stufe und die weiteren Fristen um die Dauer der Verzögerung; verweigert sie die Abnahme wegen Mängeln, bleiben die Fristen unberührt. Der Auftragnehmer zeigt die Vorlage und ihren Zeitpunkt in Textform an; die abnehmende Stelle bestätigt den Eingang. Mit dem Ablauf der Prüffrist gilt die Abnahme nicht als erteilt; der Fristablauf wirkt allein für die Verschiebung nach dem vorstehenden Satz. Im Übrigen gelten für Abnahme und Mängelrechte die werkvertraglichen Regelungen, um die der EVB-IT Dienstvertrag (Anlage 25.0) für die Stufen 1 und 2 ergänzt ist.

Die Leistungspakete nach Abschnitt 4.3 sind den Stufen nach der nachstehenden Zuordnung zugewiesen. Ein Leistungspaket kann Anteile in mehreren Stufen haben; maßgeblich für Reihenfolge und Termin ist die Stufe, nicht das Paket. Die den Stufen 1 und 2 zugewiesenen Anteile der Pakete 1 bis 3 werden nach Abschnitt 4.1 vorrangig abgerufen; eine Mindestabnahme wird auch für sie nicht vereinbart. Alle übrigen Anteile und Pakete werden auf Abruf erbracht; eine Mindestabnahme wird nicht vereinbart.

Der Auftragnehmer weist den Aufwand in Personentagen je Leistungspaket aus, bei den Paketen 1 bis 3 zusätzlich getrennt je Stufe.

Leistungspaket	Stufe 1 – Grundgerüst	Stufe 2 – Bewertungsverfahren	Stufe 3 – Betrieb und Verbesserung
Paket 1 – Aufbau des Managementsystems	Geltungsbereich, Politik, Rollen und Verantwortlichkeiten, Verzeichnis der KI-Systeme, Dokumentenlenkung	Verfahren zur Risikobeurteilung und zur Bewertung der Auswirkungen, Anbindung an das Risikoregister	Lebenszyklussteuerung, Überwachung und Verbesserung (Abruf)
Paket 2 – Richtlinien und prüfbare Vorgaben	Richtlinienrahmen und erste Zuordnung zu den Maßnahmen des Anhangs A	Ableitung von Anforderungen, Nachweisen, Rollen und Prozessen für die Bewertungsverfahren	Vorgaben für interne Audits, Managementbewertung und Lieferantensteuerung (Abruf)
Paket 3 – Musterdokumente	Vorlagen für Verzeichnis, Rollen- und Verantwortungsmatrix sowie Anwendungsfallbeschreibung und Freigabe	Vorlagen für Risikobeurteilung, Datenschutz-Folgenabschätzung, Grundrechte-Folgenabschätzung sowie Prüf- und Freigabeprotokolle	Vorlagen für interne Audits und Managementbewertung (Abruf)
Paket 4 – Anwendungsbezogene Unterstützung	—	Abruf je Einsatzfall; setzt die Verfahren der Stufe 2 voraus	Abruf je Einsatzfall
Paket 5 – Prüfung und Begleitung	—	Prüfung der Stufenergebnisse (Abruf)	Wirksamkeitsprüfung, Begleitung interner Audits, Vorbereitung auf Prüfungen durch Aufsichtsbehörden, Schulung (Abruf)
Paket 6 – Technische Sicherheitsprüfungen	Stufenunabhängig; Abruf nach Bedarf der abrufenden Stelle		
Paket 7 – Leistungen außerhalb des Managementsystems	Stufenunabhängig; Abruf nach Bedarf der abrufenden Stelle		
Paket 8 – Governance-Rahmen für die Entwicklung von KI-Systemen	Setzt den Abschluss der Stufe 1 voraus, im Übrigen stufenunabhängig; Abruf		
Paket 9 – KI-Red-Teaming	Stufenunabhängig; Abruf nach Bedarf der abrufenden Stelle		

Eine Stufe ist abgeschlossen, wenn die ihr zugewiesenen Ergebnisse übergeben und von der nach Absatz 1 zur Abnahme berufenen Stelle abgenommen sind. Die Ergebnisse je Stufe sind in Abschnitt 4.10 aufgeführt.

4.3 Leistungspakete

Die Leistung gliedert sich in die nachfolgenden Leistungspakete. Art und Umfang der Abrufleistungen richten sich nach der Zuordnung in Abschnitt 4.2. Der Auftragnehmer benennt je Paket den Aufwand in Personentagen und die eingesetzten Qualifikationen.

Paket 1: Aufbau des Managementsystems. Festlegung von Geltungsbereich, Politik, Rollen und Verantwortlichkeiten, Verfahren zur Risikobeurteilung, Verfahren zur Bewertung der Auswirkungen von KI-Systemen, Lebenszyklussteuerung, Überwachung und Verbesserung sowie der zugehörigen Dokumentenlenkung, jeweils abgebildet in der nach Abschnitt 4.1 maßgeblichen Umgebung und erbracht in dem der jeweiligen Stufe nach Abschnitt 4.2 zugewiesenen Umfang; Lebenszyklussteuerung, Überwachung und Verbesserung sind danach der Stufe 3 zugeordnet. Ist ein Bedarfsträger Betreiber einer kritischen Anlage und sind die vom Managementsystem erfassten Systeme oder Prozesse für deren Funktionsfähigkeit maßgeblich, werden die daraus folgenden Anforderungen bei der Ausgestaltung berücksichtigt. Die abschließende Bewertung und Entscheidung über die Ergebnisse der Beratungsleistung verbleibt beim Auftraggeber und beim jeweiligen Bedarfsträger; eine Verlagerung der Verantwortung auf den Auftragnehmer findet nicht statt.

Paket 2: Richtlinien und prüfbare Vorgaben. Bereitstellung von Richtlinien auf Grundlage der Norm DIN EN ISO/IEC 42001 und Anpassung an die Organisation des Auftraggebers beziehungsweise, bei einem eigenen Abruf eines Bedarfsträgers, an dessen Organisation sowie Ableitung konkreter Anforderungen, Nachweise, Rollen und Prozesse aus den in Abschnitt 3.1 genannten Regelwerken, jeweils mit Zuordnung zu den Maßnahmen des Anhangs A der Norm.

Paket 3: Musterdokumente. Erstellung wiederverwendbarer Vorlagen, insbesondere für Anwendungsfallbeschreibung und Freigabe, Risikobeurteilung, Datenschutz-Folgenabschätzung, Grundrechte-Folgenabschätzung nach Art. 27 der KI-Verordnung, soweit für den jeweiligen Einsatz erforderlich, Verzeichnis der KI-Anwendungen, Rollen- und Verantwortungsmatrix sowie Prüf- und Freigabeprotokolle.

Die Pakete 2 und 3 können auch abgerufen werden, soweit die Lösung des Fachloses 3 Leitlinien, Richtlinien oder Vorlagen zu denselben Gegenständen mitliefert. Ob deren Reifegrad für die Anforderungen der abrufenden Stelle ausreicht, entscheidet diese; die Auftragnehmer der Fachlose 2 und 3 haben hierauf keinen Einfluss.

Paket 4: Anwendungsbezogene Unterstützung. Erstellung oder Prüfung der Unterlagen für einzelne KI-Anwendungen, insbesondere Datenschutz-Folgenabschätzung, Risikobeurteilung, Einordnung nach der KI-Verordnung und Anmeldeunterlagen für die abrufende Stelle.

Paket 5: Prüfung und Begleitung. Prüfung der Wirksamkeit des Managementsystems durch Personen, die an den geprüften Arbeitsergebnissen nicht mitgewirkt haben und organisatorisch von deren Erstellung getrennt sind; die Unabhängigkeit ist zu dokumentieren. Begleitung interner Audits, Vorbereitung auf Prüfungen durch Aufsichtsbehörden sowie Schulung der beteiligten Rollen.

Paket 6: Technische Sicherheitsprüfungen. Durchführung von Penetrationstests und technischen Sicherheitsprüfungen an der Lösung des Fachloses 1 sowie an weiteren Anwendungen des Auftraggebers oder des jeweils abrufenden Bedarfsträgers, die Komponenten der künstlichen Intelligenz einsetzen, einschließlich ihrer Schnittstellen und Betriebsumgebungen, jeweils im Auftrag und im Namen der abrufenden Stelle. Prüfungen an Anwendungen ohne Bezug zu Komponenten der künstlichen Intelligenz sind nicht Gegenstand dieses Pakets; hierfür bestehen gegebenenfalls andere Vertragsgrundlagen der abrufenden Stelle. Prüfungen erfolgen ausschließlich auf Grundlage einer Beauftragung in Textform, die Prüfgegenstand, Prüfziele, zugelassene Verfahren und Prüfzeitfenster benennt. Berührt eine Prüfung Systeme Dritter, wird sie erst nach deren Zustimmung durchgeführt. Der Auftragnehmer erlangt keine über den Prüfzweck hinausgehenden Rechte; erlangte Daten werden

ausschließlich für den Prüfbericht verwendet, nicht weitergegeben und nach Abschluss der Prüfung gelöscht. Festgestellte Schwachstellen werden unverzüglich und vertraulich an die abrufende Stelle berichtet. Die Prüfungen an der Lösung des Fachloses 1 schließen die gemeinsam genutzten Infrastrukturbestandteile ein.

Paket 7: Leistungen außerhalb des Managementsystems. Beratungs- und Unterstützungsleistungen zu Governance, Informationssicherheit und Datenschutz im Zusammenhang mit KI-Anwendungen zu den im Angebot benannten Tagessätzen. Der Abruf erfolgt nach der Rahmenvereinbarung (Anlage 26.2); die abrufende Stelle bestimmt mit dem Abruf den Umfang. Die Leistungen werden auf den Höchstwert nach Abschnitt 4.1 angerechnet.

Paket 8: Governance-Rahmen für die Entwicklung von KI-Systemen. Unterstützung bei der Erstellung eines Rahmens für die Entwicklung eigener KI-Systeme beim Auftraggeber und bei den Bedarfsträgern, insbesondere zu Zuständigkeiten, Freigabestufen, Anforderungen an Daten und Modelle, Prüf- und Dokumentationspflichten sowie zur Abgrenzung gegenüber der Beschaffung fertiger Lösungen.

Paket 9: KI-Red-Teaming. Gezielte, szenariobasierte Angriffe auf die Lösung des Fachloses 1 und auf weitere Anwendungen des Auftraggebers oder des jeweils abrufenden Bedarfsträgers, die Komponenten der künstlichen Intelligenz einsetzen, um die Wirksamkeit der Schutzmechanismen unter realistischen Bedingungen zu prüfen, insbesondere gegen die Angriffsklassen nach Abschnitt 4.6. Für Beauftragung, Rechtsrahmen, Umgang mit erlangten Daten und Berichterstattung gelten die Regelungen des Pakets 6 entsprechend; die eingesetzten Personen erfüllen das Profil des Security Consultant und Penetrationstesters nach Abschnitt 4.6. Das Paket wird auf Abruf erbracht; eine feste Beauftragung und eine Mindestabnahme werden nicht vereinbart.

4.4 Abgrenzung zu Fachlos 1

Der Auftragnehmer des Fachloses 2 erhält keine Weisungsbefugnis gegenüber dem Auftragnehmer des Fachloses 1. Empfehlungen und Feststellungen aus Fachlos 2 binden den Auftragnehmer des Fachloses 1 erst, wenn der Auftraggeber sie nach dem für Fachlos 1 geregelten Änderungsverfahren als Änderung verlangt.

Vorgaben aus Fachlos 2 gehen inhaltlich nicht über die in Abschnitt 3.1 genannten Regelwerke hinaus. Ein eigenständiges, von diesen Regelwerken abweichendes Anforderungswerk wird nicht erstellt.

Der Auftragnehmer des Fachloses 2 wertet die vom Auftragnehmer des Fachloses 1 zur KI-Governance gelieferten Angaben und Unterlagen aus und zeigt der abrufenden Stelle auf, welche Anforderungen des Managementsystems damit abgedeckt sind und wo Lücken bestehen; ist das gemeinschaftliche Managementsystem betroffen, zeigt er dies dem Auftraggeber auf.

Zur Abgrenzung gegenüber der Rechtsberatung gilt Abschnitt 11.5.

4.5 Anforderungen an den Auftragnehmer

Der Auftragnehmer verfügt über nachgewiesene Erfahrung im Aufbau von Managementsystemen für Informationssicherheit sowie über Kenntnisse der Verordnung über künstliche Intelligenz und des Sozialdatenschutzes. Die Leistung wird durch Personen mit einschlägiger Berufserfahrung erbracht.

Für die Verarbeitung von Sozial- und Gesundheitsdaten sowie für Personalsicherheit und Vertraulichkeit gilt Kapitel 11.

Für die Rechte an den Arbeitsergebnissen gelten der EVB-IT Dienstvertrag (Anlage 25.0) und die EVB-IT Dienstleistungs-AGB (Anlage 25.1). Zu übergeben sind insbesondere Konzepte, Vorgaben, Musterdokumente und Prüfberichte, jeweils in bearbeitbarer und, soweit maschinelle Weiterverarbeitung in Betracht kommt, in strukturierter und maschinenlesbarer Form.

4.6 Qualifikation des eingesetzten Personals

Die Leistungen des Fachloses 2 sind durch Personen zu erbringen, die die nachstehenden Mindestanforderungen erfüllen. Der Auftragnehmer benennt je Profil die vorgesehenen Personen mit Qualifikation, Zertifizierungen und Referenzprojekten. Die im Angebot benannten und bewerteten Personen sind für die Leistungserbringung einzusetzen; ein Austausch ist nur mit vorheriger Zustimmung des Auftraggebers und nur gegen Personen zulässig, die mindestens gleichwertig qualifiziert sind. Eine Person, die für das Fachlos 2 benannt ist, darf nicht zugleich für das Fachlos 1 oder für das Fachlos 3 benannt werden; die Prüf- und Red-Teaming-Leistungen des Fachloses 2 erfassen nach Abschnitt 4.3 auch weitere Anwendungen mit Komponenten der künstlichen Intelligenz und damit die Lösung des Fachloses 3, sobald deren Funktionen nach den für Fachlos 3 geltenden Regelungen aktiviert sind. Für die Fachlose 1 und 3 ist die Benennung derselben Person zulässig, soweit die zugesagte Verfügbarkeit gewahrt bleibt.

Senior Consultant Informationssicherheit und KI-Governance, mindestens zwei Personen: mindestens acht Jahre Berufserfahrung im Aufbau, Betrieb oder in der Prüfung von Managementsystemen für Informationssicherheit. Zusätzlich ist für mindestens eine der benannten Personen ein aktueller Bezug zur Norm DIN EN ISO/IEC 42001 und zur KI-Verordnung nachzuweisen, wahlweise durch ein abgeschlossenes oder laufendes Projekt zum Aufbau eines Managementsystems für künstliche Intelligenz, durch eine einschlägige Zertifizierung oder durch eine vergleichbare Befassung. Eine Mindestdauer der Berufserfahrung wird hierfür nicht verlangt.

Senior Consultant Datenschutz und Sozialdatenschutz, mindestens eine Person: mindestens acht Jahre Berufserfahrung im Datenschutzrecht, davon einschlägige Erfahrung im Sozialdatenschutz nach dem Zehnten Buch Sozialgesetzbuch. Nachzuweisen sind Datenschutz-Folgenabschätzungen, die nach Geltungsbeginn der Verordnung (EU) 2016/679 erstellt wurden, sowie Erfahrung mit der Auftragsverarbeitung nach § 80 des Zehnten Buches Sozialgesetzbuch. Darzulegen ist ferner die Befassung mit den Anforderungen an die Nutzung von Cloud-Diensten in der Sozialversicherung, insbesondere nach § 393 des Fünften Buches Sozialgesetzbuch und den hierzu ergangenen Anforderungen des Bundesamts für Soziale Sicherung.

Security Consultant und Penetrationstester, mindestens eine Person: mindestens fünf Jahre Berufserfahrung in der technischen Sicherheitsprüfung von Anwendungen und Schnittstellen, nachgewiesen durch Referenzprojekte. Nachzuweisen ist eine anerkannte Prüferzertifizierung, zum Beispiel OSCP, OSEP, CREST CRT oder CREST CCT, GIAC GPEN oder GIAC GWAPT oder die Zertifizierung als IS-Penetrationstester durch das Bundesamt für Sicherheit in der Informationstechnik, jeweils oder gleichwertig. Die eingesetzte Person weist zusätzlich Kenntnisse und praktische Erfahrung in der Sicherheitsprüfung von Anwendungen nach, die Sprachmodelle oder vergleichbare Komponenten der künstlichen Intelligenz einsetzen. Die Kenntnisse erstrecken sich mindestens auf die Übernahme von Anweisungen aus Dokumenten und anderen nicht vertrauenswürdigen Inhalten, die Manipulation von Abruf und Kontextbildung einschließlich der Quellenzuordnung, die Trennung von Fällen, Mandanten und Sitzungen einschließlich einer Offenlegung über Protokolle, Fehlermeldungen und Telemetrie, die Prüfung von Werkzeug- und Schnittstellenaufrufen einschließlich Auflösung, Parameterprüfung und Begrenzung der Systemwirkung sowie die Umgehung von Schutz- und Überwachungsmechanismen durch mehrstufige Vorgehensweisen. Der Nachweis kann durch ein einschlägiges Referenzprojekt, eine nachvollziehbare eigene Prüfmethodik, eine veröffentlichte Untersuchung, entwickelte reproduzierbare Testfälle oder eine vergleichbare praktische Leistung erbracht werden; aus ihm müssen Untersuchungsgegenstand, Rolle der Person, geprüfte Angriffsklassen und Art der Ergebnisdokumentation hervorgehen. Das Erreichen der vorstehenden Mindestanforderungen ist Voraussetzung für die Berücksichtigung des Profils. Umfang, Vergleichbarkeit und methodische Tiefe der darüber hinaus nachgewiesenen Erfahrung werden nach Maßgabe der Vergabeunterlagen bewertet.

Das Profil des Security Consultant und Penetrationstesters kann durch einen Unterauftragnehmer oder eine freiberuflich tätige Person gestellt werden. Mit dem Angebot ist nachzuweisen, dass der Bieter die Prüfleistung erbringen kann; benennt er hierfür einen Dritten, legt er dessen Verpflichtungserklärung nach § 47 der Vergabeverordnung vor, mit der dieser die Bereitstellung der erforderlichen Mittel zusagt.

Beim Abruf einer Prüfung benennt der Auftragnehmer die konkret eingesetzte Person und weist nach, dass sie die Anforderungen dieses Abschnitts erfüllt. Handelt es sich um eine andere Person oder einen anderen Dritten als im Angebot benannt, bedarf der Einsatz der vorherigen Zustimmung des Auftraggebers; sie wird erteilt, wenn die Person die Anforderungen dieses Abschnitts erfüllt und mindestens gleichwertig qualifiziert ist wie die im Angebot benannte Person. Im Übrigen richtet sich der Einsatz von Unterauftragnehmern und freiberuflich Tätigen nach dem Einzelvertrag (EVB-IT Dienstvertrag, Anlage 25.0).

Für eingesetzte Dritte gelten die Vertraulichkeitsverpflichtung, die Anforderungen an die Zuverlässigkeit sowie der Rechtsrahmen für Prüfungen nach Abschnitt 4.3 in gleicher Weise. Der Auftragnehmer gibt diese Pflichten vertraglich weiter und bleibt gegenüber der jeweils abrufenden Stelle allein verantwortlich.

Consultant Informationssicherheit und Datenschutz, mindestens zwei Personen: mindestens drei Jahre Berufserfahrung im relevanten Tätigkeitsfeld. Personen dieses Profils werden ausschließlich unterstützend und unter fachlicher Verantwortung des für die jeweilige Leistung einschlägigen Seniorprofils eingesetzt; bei Leistungen des Datenschutzes und des Sozialdatenschutzes ist dies das entsprechende Seniorprofil, bei Leistungen der Informationssicherheit und der KI-Governance das dortige. Die Erstellung von Datenschutz-Folgenabschätzungen, Risikobeurteilungen und Prüfberichten ist ihnen nicht übertragbar.

Erfahrung ist ein durch praktische Tätigkeit oder Befassung mit entsprechenden Projekten erworbener Wissensstand. Bezieht sich eine Anforderung auf ein Regelwerk, das erst kürzlich in Kraft getreten oder veröffentlicht worden ist, tritt an die Stelle einer Mindestdauer der Nachweis einer einschlägigen Befassung. Alle für die Leistung vorgesehenen Personen beherrschen die deutsche Sprache nachweislich mindestens im Niveau B2 nach dem Gemeinsamen Europäischen Referenzrahmen für Sprachen; mindestens die Hälfte dieser Personen beherrscht sie im Niveau C1.

4.7 Projektkoordination

Der Auftragnehmer benennt einen Projektkoordinator, der Arbeitsnachweise, Arbeits- und Personalorganisation sowie vertragsbezogene Themen mit der abrufenden Stelle abstimmt. Der Projektkoordinator verfügt über mindestens drei Jahre Erfahrung in der Leitung von Beratungsprojekten und beherrscht die deutsche Sprache im Niveau C1. Er steht montags bis freitags von 8:00 bis 17:00 Uhr zur Verfügung, ausgenommen bundeseinheitliche Feiertage.

4.8 (entfallen)

Abruf, Leistungsnachweis, Abrechnung, Abnahme und Preisanpassung regeln die Rahmenvereinbarung (Anlage 26.2) und der Einzelvertrag.

4.9 (entfallen)

4.10 Zu übergebende Ergebnisse

Je Stufe nach Abschnitt 4.2 zu übergeben sind die dieser Stufe zugewiesenen Ergebnisse: für Stufe 1 Geltungsbereich, Politik, Rollen- und Verantwortungsmatrix, Verzeichnis der KI-Systeme, Dokumentenlenkung sowie der Richtlinienrahmen mit der Zuordnung zu den Maßnahmen des Anhangs A der Norm DIN EN ISO/IEC 42001; für Stufe 2 die Verfahren zur Risikobeurteilung und zur Bewertung der Auswirkungen, die Anbindung an das Risikoregister sowie die zugehörigen Musterdokumente; für Stufe 3 die Verfahren für Überwachung, interne Audits, Managementbewertung, Verbesserung, Lieferantensteuerung und Lebenszyklussteuerung. Für die Abnahme gilt der letzte Absatz dieses Abschnitts.

Im Verlauf der Leistungserbringung zu übergeben sind: das Managementsystem einschließlich Politik, Verfahren, Rollen und Dokumentenlenkung, abgebildet in der nach Abschnitt 4.1 maßgeblichen Umgebung; die Richtlinien und Musterdokumente nach Abschnitt 4.3; die Zuordnung der Anforderungen zu den Maßnahmen des Anhangs A der Norm DIN EN ISO/IEC 42001; sowie die Ergebnisse und Prüfberichte der Prüfungen nach den Paketen 5, 6 und 9; je Bedarfsträger und Einsatzfall eine Einstufungs- und Freigabeakte mit der Risikobeurteilung, der Einordnung nach der Verordnung (EU) 2024/1689, der Prüfung, ob eine Datenschutz-Folgenabschätzung oder eine Grundrechte-Folgenabschätzung erforderlich ist, und der dokumentierten Freigabeentscheidung; die Entscheidung selbst trifft der jeweilige Bedarfsträger; bei Abruf des Pakets 8 der Governance-Rahmen für die Entwicklung von Systemen der künstlichen Intelligenz nach Abschnitt 4.3.

Die Abnahme der Leistungsanteile der Stufen 1 und 2 erfolgt jeweils nach Abschluss der Stufe nach Maßgabe des Abschnitts 4.2 und der werkvertraglichen Ergänzung des EVB-IT Dienstvertrags (Anlage 25.0). Leistungsanteile der Stufe 3 und sonstige Abrufleistungen werden abgenommen, soweit für sie

ein Festpreis vereinbart ist; die Abnahme richtet sich dann nach dem jeweiligen Einzelauftrag anhand der dort festgelegten Ergebnisse und nach der werkvertraglichen Ergänzung des EVB-IT Dienstvertrags (Anlage 25.0). Für dienstvertraglich vereinbarte Abrufleistungen gilt der Leistungsnachweis nach § 10 Abs. (6) der Rahmenvereinbarung (Anlage 26.2).

Teil III – Gemeinsame Bestimmungen

5 Geltungsbereich der gemeinsamen Bestimmungen

Die Kapitel dieses Teils gelten für den Auftragnehmer dieses Fachloses. Sie beschreiben die Anforderungen an seine Zugänge, an die ihm überlassenen Unterlagen, an seine Arbeitsmittel und an seine Arbeitsergebnisse.

Anforderungen an Komponenten, Betrieb und Datenhaltung eines vom Auftragnehmer betriebenen Dienstes sind nicht Gegenstand dieses Fachloses und in diesem Dokument nicht enthalten.

5.1 Geltungsbereich und Schutzbedarf

(1) Die Anforderungen der Kapitel 5 bis 10 gelten für die Zugänge, die überlassenen Unterlagen, die Arbeitsmittel und die Arbeitsergebnisse des Auftragnehmers.

(2) Sie gelten gleichermaßen für alle Unterauftragnehmer und freiberuflich Tätigen, die personenbezogene Daten, Sozialdaten oder Gesundheitsdaten verarbeiten oder auf sie zugreifen können. Der Auftragnehmer stellt die Weitergabe der Verpflichtungen vertraglich sicher.

(3) Der Schutzbedarf der verarbeiteten Daten ist in den Schutzzielen Vertraulichkeit, Integrität und Verfügbarkeit als hoch einzustufen. Maßnahmen sind an diesem Schutzbedarf auszurichten.

(4) Für das Informationssicherheitsmanagement des Auftragnehmers ist die Norm DIN EN ISO/IEC 27001 maßgeblich; ergänzend gelten die vom Auftraggeber vorgegebenen Sicherheitsanforderungen, jeweils in der geltenden Fassung. Der Auftraggeber unterhält für den Einsatz von Systemen der künstlichen Intelligenz ein eigenes Managementsystem in Anlehnung an die Norm DIN EN ISO/IEC 42001. Eine eigene Zertifizierung des Auftragnehmers nach DIN EN ISO/IEC 42001 ist nicht gefordert.

(5) Die anwendbaren Regelwerke sind in Abschnitt 3.1 aufgeführt; die Kapitel dieses Teils konkretisieren die daraus folgenden Anforderungen für dieses Fachlos.

(6) Maßgeblich ist der Stand der Technik im Zeitpunkt der jeweiligen Leistungserbringung, nicht im Zeitpunkt des Vertragsschlusses. Werden in dieser Leistungsbeschreibung Normen, Technische Richtlinien oder Standards genannt, gelten sie in der jeweils geltenden Fassung. Der Auftragnehmer beobachtet deren Fortschreibung und zeigt dem Auftraggeber daraus folgenden Anpassungsbedarf unaufgefordert an. Die Anpassung an den fortgeschriebenen Stand der Technik ist Teil der geschuldeten Leistung, soweit sie den bestehenden Leistungsumfang erhält. Erfordert eine geänderte Vorgabe einen wesentlichen Zusatzaufwand, so wird er nach dem im Rahmenvertrag geregelten Verfahren vereinbart.

(7) Nachweise, Konzepte und Erklärungen nach den Kapiteln 5 bis 10 werden einmalig auf Ebene der Rahmenvereinbarung erbracht und je Abruf um die abrufspezifischen Angaben ergänzt. Eine erneute vollständige Vorlage je Abruf ist nicht erforderlich.

6 Zugänge, Unterlagen und Arbeitsmittel

6.1 Identitäts- und Berechtigungsmanagement

Für die Zugänge, die der Auftragnehmer beim Auftraggeber oder bei einem abrufenden Bedarfsträger erhält, gelten die nachstehenden Anforderungen.

Zugänge werden personenbezogen eingerichtet; eine gemeinsame Nutzung durch mehrere Personen ist ausgeschlossen. Die Anmeldung erfolgt mit einem Mehrfaktorverfahren.

Rechte werden nach dem Grundsatz der Erforderlichkeit vergeben. Scheidet eine Person aus der Leistungserbringung aus, wird ihr Zugang unverzüglich entzogen; der Auftragnehmer zeigt das Ausscheiden unverzüglich an.

Für technische Konten, die der Auftragnehmer für seine Arbeitsmittel benötigt, werden kurzlebige, an den jeweiligen Vorgang gebundene Zugangsmittel verwendet, soweit die eingesetzten Verfahren dies zulassen. Dauerhaft hinterlegte Zugangsdaten werden vermieden; ihre Verwendung ist zu begründen und von der Stelle freizugeben, in deren Verantwortungsbereich sie eingesetzt werden.

Die abrufende Stelle kann die dem Auftragnehmer eingeräumten Berechtigungen jederzeit auswerten und überprüfen. Der Auftragnehmer wirkt daran mit und führt die Liste der eingesetzten Personen nach Abschnitt 8.2.

6.2 Aufbewahrung und Löschung überlassener Unterlagen

Der Auftragnehmer bewahrt überlassene Unterlagen und die daraus erstellten Arbeitsergebnisse nur so lange auf, wie es für die Erbringung des jeweiligen Einzelauftrags erforderlich ist.

Nach Abschluss eines Einzelauftrags werden die überlassenen Unterlagen gelöscht oder zurückgegeben, spätestens dreißig Werktage nach dessen Abschluss; für die Arbeitsergebnisse gilt Abschnitt 9.2. Gesetzliche Aufbewahrungspflichten bleiben unberührt.

Die Löschung wird dokumentiert und auf Verlangen nachgewiesen.

6.3 Fernzugang

Arbeitet der Auftragnehmer über einen Fernzugang, wird dieser von der abrufenden Stelle bereitgestellt und ist auf die für den Einzelauftrag erforderlichen Systeme beschränkt.

Fernzugriffe erfolgen ausschließlich über von der abrufenden Stelle freigegebene Verfahren, verschlüsselt, mehrfaktorauthentisiert und zeitlich begrenzt.

Fernzugriffe werden im Einzelfall freigegeben oder dauerhaft geregelt; zuständig ist die Stelle, in deren Verantwortungsbereich zugegriffen wird. Sie kann laufende Sitzungen jederzeit unterbrechen.

Endgeräte, mit denen der Auftragnehmer über einen Fernzugang arbeitet, unterliegen definierten Anforderungen an Verschlüsselung, Patchstand und Schadsoftwareschutz und werden nicht für private Zwecke genutzt.

Fernzugänge werden vollständig protokolliert. Der Auftraggeber und der betroffene Bedarfsträger können Sitzungen mitverfolgen.

Eine Ausleitung von Daten des Auftraggebers oder der Bedarfsträger aus einer solchen Sitzung erfolgt nur mit vorheriger Zustimmung der Stelle, in deren Verantwortungsbereich die Daten liegen, und zusätzlich des Auftraggebers; sie wird protokolliert.

Eigene Zugangswege des Auftragnehmers in Systeme der abrufenden Stelle sind unzulässig.

7 Protokollierung

7.1 Protokollierung und Beweissicherung

Zugriffe des Auftragnehmers auf Systeme und Unterlagen des Auftraggebers oder eines abrufenden Bedarfsträgers werden protokolliert.

Je Ereignis werden mindestens erfasst: Zeitpunkt, handelnde Person, betroffenes System, betroffene Unterlage und ausgelöste Funktion. Bei administrativen Zugriffen werden zusätzlich Zweck und Auftragsbezug erfasst.

Protokolle enthalten keine Dokumentinhalte und keine Gesundheitsdaten. Wo ein Inhaltsbezug erforderlich ist, erfolgt er über Kennungen und Fundstellenverweise.

Die Protokolle sind gegen Veränderung geschützt. Bei einem Sicherheitsvorfall stellt der Auftragnehmer die für die Aufklärung erforderlichen Protokolle unverzüglich bereit.

Die Protokolle werden bis zu zwölf Monate aufbewahrt. Die Aufbewahrungsdauer legt die abrufende Stelle je Protokollart fest; eine längere Aufbewahrung ist nur bei besonderem, dokumentiertem Bedarf und auf Weisung der verantwortlichen Stelle zulässig. Der Auftragnehmer benennt die Protokollarten je eingesetztem Arbeitsmittel; diese Angabe ist Bezugsgröße für die Festlegung der Aufbewahrungsdauer und für die Prüfung der Nachweise.

8 Sichere Arbeitsweise und Vorfälle

8.1 Überlassene Test-, Schulungs- und Entwicklungsdaten

Werden dem Auftragnehmer Test-, Schulungs- oder Entwicklungsdaten überlassen, verarbeitet er sie ausschließlich für den jeweiligen Einzelauftrag.

In Schulungs-, Entwicklungs- und Demonstrationsumgebungen werden keine Echtdaten verarbeitet. In Testumgebungen dürfen Echtdaten nur zur Reproduktion eines konkreten Fehlers oder zur

technischen Validierung verarbeitet werden, jeweils nur auf ausdrückliche, dokumentierte Weisung der für die Verarbeitung verantwortlichen Stelle, auf gesonderter Rechtsgrundlage, beschränkt auf den erforderlichen Umfang, zeitlich befristet und mit anschließender Löschung. Die Dauer der Befristung gibt die weisende Stelle vor; mit Wegfall des Zwecks werden die Daten unverzüglich gelöscht.

Ohne eine solche Weisung sind ausschließlich synthetische oder wirksam anonymisierte Daten zu verwenden. Eine Pseudonymisierung genügt nicht.

Solange Umgebungen Echtdaten enthalten, unterliegen sie demselben Schutzniveau wie die Produktivsysteme der abrufenden Stelle, einschließlich Zugriffskontrolle, Verschlüsselung, Protokollierung und Netztrennung.

Die Entscheidung über den Einsatz von Echtdaten trifft die abrufende Stelle und dokumentiert sie.

Nach Abschluss von Test-, Schulungs- oder Entwicklungstätigkeiten werden Echtdaten aus den betreffenden Umgebungen einschließlich Sicherungen gelöscht. Die Löschung wird nachgewiesen.

Nach Abschluss des Einzelauftrags gilt im Übrigen Abschnitt 6.2.

8.2 Personalsicherheit und Vertraulichkeit

Personalsicherheit im Sinne dieses Abschnitts umfasst die personenbezogenen Maßnahmen vor, während und nach einer Tätigkeit im Sinne der Maßnahmen zur Personalsicherheit nach der Norm DIN EN ISO/IEC 27001. Der Auftragnehmer verpflichtet alle Personen, die Zugang zu Daten oder Systemen des Auftraggebers oder eines Bedarfsträgers erhalten können, vor Aufnahme der Tätigkeit schriftlich auf die Wahrung der Vertraulichkeit und auf das Sozialgeheimnis nach § 35 SGB I in Verbindung mit § 78 SGB X. Die Verpflichtung wirkt über das Ende der Tätigkeit hinaus fort.

Alle Personen, die Zugang zu Daten oder Systemen des Auftraggebers oder eines Bedarfsträgers erhalten, werden vor der ersten Tätigkeit und danach wiederkehrend zu Informationssicherheit, Sozialdatenschutz und zum Umgang mit KI-Komponenten geschult. Der Auftragnehmer weist die Durchführung auf Verlangen nach.

Für Personen mit administrativem Zugriff oder mit Zugriff auf Sozial- und Gesundheitsdaten führt der Auftragnehmer eine dokumentierte Zuverlässigkeitsprüfung nach einem festgelegten Verfahren durch und weist das Verfahren auf Verlangen nach.

Der Auftragnehmer unterhält ein Verfahren, das bei Ausscheiden oder Aufgabenwechsel den unverzüglichen Entzug sämtlicher Zugänge, die Rückgabe von Berechtigungsmitteln und die Deaktivierung von Konten sicherstellt.

Der Auftragnehmer führt eine aktuelle Liste der Personen mit Zugriffsmöglichkeit auf Systeme oder Daten des Auftraggebers und der Bedarfsträger einschließlich der Personen bei Unterauftragnehmern und stellt sie dem Auftraggeber auf Verlangen bereit.

Anforderungen, die den Betrieb eines Dienstes betreffen, insbesondere zur Trennung von Betriebs- und Administrationsrollen, gelten für dieses Fachlos nicht.

8.3 Sichere Entwicklung, Schwachstellen und Lieferkette

Der Auftragnehmer setzt für die Leistungserbringung nur Arbeitsmittel und Prüfwerkzeuge ein, die auf einem gepflegten Stand sind und für die der Hersteller Sicherheitskorrekturen bereitstellt.

Für eigene Konfigurationen, Skripte und Prüfwerkzeuge gilt ein dokumentiertes Entwicklungs- und Freigabeverfahren; Änderungen werden nachvollziehbar festgehalten.

Vor dem Einsatz eines Prüfwerkzeugs an Systemen der abrufenden Stelle stimmt er Werkzeug, Verfahren und Prüffenster mit ihr ab.

Werden bei der Leistungserbringung Schwachstellen bekannt, die Daten der abrufenden Stelle betreffen können, zeigt der Auftragnehmer dies unverzüglich an.

8.4 Sicherheitsvorfälle

(1) Der Auftragnehmer meldet Sicherheits- und Datenschutzvorfälle unverzüglich, spätestens innerhalb von zwölf Stunden ab Kenntnis an den jeweils betroffenen Bedarfsträger; der Auftraggeber und die von ihm benannte zentrale Stelle werden zusätzlich unterrichtet, soweit die Leistungen zum gemeinschaftlichen Managementsystem, mehrere Bedarfsträger oder die gemeinsame Sicherheitskoordination betroffen sind. Die Frist ist so bemessen, dass die jeweils betroffenen Bedarfsträger sowie, soweit einschlägig, der Auftraggeber ihre gesetzlichen und vertraglichen Melde-, Anzeige- und Frühwarnpflichten fristgerecht erfüllen können.

(2) Betrifft ein Vorfall oder ein hierauf hindeutendes Ereignis die Informationssicherheit mehrerer Bedarfsträger, unterrichtet der Auftragnehmer den Auftraggeber unverzüglich und gesondert, damit dieser die von ihm hierfür bestimmte Stelle einbinden kann. Der Auftragnehmer wirkt an deren Aufklärung und Bewältigung mit.

(3) Auf die Erstmeldung folgen eine vollständige Meldung innerhalb von 72 Stunden und ein Abschlussbericht innerhalb eines Monats nach Abschluss der Bearbeitung. Die Meldungen enthalten Zeitpunkt, betroffene Komponenten und Datenkategorien, Auswirkungsanalyse, Sofortmaßnahmen, Ansprechpartner und geplante weitere Maßnahmen.

(4) Der Auftragnehmer unterhält ein dokumentiertes Verfahren zur Vorfallbehandlung, benennt eine erreichbare Kontaktstelle und wirkt an der Aufklärung mit, einschließlich der Bereitstellung von Protokollen und forensisch verwertbaren Informationen.

(5) Der Auftragnehmer unterrichtet die jeweils betroffenen Bedarfsträger unverzüglich über Vorfälle bei Unterauftragnehmern, soweit deren Verarbeitung oder Leistung betroffen sein kann. Der Auftraggeber und die von ihm benannte zentrale Stelle werden zusätzlich unterrichtet, soweit die Leistungen zum gemeinschaftlichen Managementsystem, mehrere Bedarfsträger oder die gemeinsame Sicherheitskoordination betroffen sind.

(6) Die Meldepflichten treffen jeden Auftragnehmer für den von ihm verantworteten Leistungsteil. Der Auftragnehmer benennt eine Stelle, die Meldungen für alle abrufenden Bedarfsträger entgegennimmt und weitergibt. Betrifft ein Vorfall mehrere abrufende Bedarfsträger, unterrichtet der Auftragnehmer alle betroffenen Bedarfsträger sowie die vom Auftraggeber benannte zentrale Stelle. Die Unterrichtung der zentralen Stelle ersetzt nicht die Meldung an den betroffenen Bedarfsträger.

9 Prüfrechte und Vertragsende

9.1 Prüfrechte, wiederkehrende Überprüfung und Betriebsdokumentation

Die abrufende Stelle ist berechtigt, die Einhaltung der für dieses Fachlos geltenden Anforderungen zu überprüfen, auch durch beauftragte Dritte. Die Prüfung erfolgt mindestens einmal jährlich sowie anlassbezogen und kann dokumentenbasiert oder vor Ort durchgeführt werden.

Die Prüfung erstreckt sich auch auf eingesetzte Unterauftragnehmer und freiberuflich Tätige.

Der Auftragnehmer wirkt an der Überprüfung mit und legt die hierfür erforderlichen Unterlagen vor, insbesondere Nachweise zu Qualifikation, Verpflichtung und Schulung der eingesetzten Personen sowie zur Löschung überlassener Unterlagen.

Der Auftragnehmer unterrichtet den Auftraggeber und den betroffenen Bedarfsträger vor einer Kommunikation mit Aufsichtsbehörden, soweit sie die Leistung betrifft, und führt keine eigenständige Korrespondenz mit der für den Auftraggeber oder den jeweiligen Bedarfsträger zuständigen Aufsicht. Dies gilt nicht, soweit eine ihn unmittelbar treffende gesetzliche Verpflichtung entgegensteht; in diesem Fall beschränkt er die Kommunikation auf das gesetzlich Erforderliche und unterrichtet den Auftraggeber und den betroffenen Bedarfsträger unverzüglich, soweit ihm das rechtlich möglich ist.

Eine Betriebsdokumentation ist nicht vorzulegen.

9.2 Datenrückgabe, Löschung und technische Übergabe bei Vertragsende

Mit Abschluss des jeweiligen Einzelauftrags, spätestens mit Vertragsende, gibt der Auftragnehmer die überlassenen Unterlagen zurück und löscht verbliebene Kopien einschließlich der Bestände in Sicherungen und bei Unterauftragnehmern.

Vorhandene administrative Zugänge werden deaktiviert.

Die Arbeitsergebnisse werden in bearbeitbarer und, soweit maschinelle Weiterverarbeitung in Betracht kommt, in strukturierter und maschinenlesbarer Form übergeben.

Die Löschung wird nachgewiesen. Gesetzliche Aufbewahrungspflichten bleiben unberührt.

10 Einsatz von Komponenten der künstlichen Intelligenz

Dieses Kapitel gilt, soweit der Auftragnehmer bei der Leistungserbringung selbst Komponenten der künstlichen Intelligenz einsetzt.

10.1 Grundsätze für den Einsatz

Der Auftragnehmer verarbeitet überlassene Inhalte nicht in Systemen der künstlichen Intelligenz, die er selbst betreibt oder durch Dritte betreiben lässt, insbesondere nicht zu Zwecken des Trainings oder der Produktverbesserung.

Dies gilt nicht für Werkzeuge, deren Anbieter vertraglich ausschließt, dass eingegebene Inhalte zu eigenen Zwecken verwendet werden, insbesondere für Training, Feinabstimmung, bestärkendes Lernen, Evaluierung, Vergleichsmessungen, Produktverbesserung oder eine nicht auftragsbezogene Missbrauchserkennung, dass sie über die für die konkrete Bearbeitung erforderliche Dauer hinaus gespeichert werden und dass Personen des Anbieters Einsicht in sie nehmen. Der Auftragnehmer weist dies auf Verlangen nach.

Werden solche Werkzeuge an Unterlagen eingesetzt, die Sozialdaten enthalten, bedarf dies der vorherigen Zustimmung der abrufenden Stelle. Die Zustimmung setzt voraus, dass die datenschutzrechtlichen Voraussetzungen für die Einbeziehung des Werkzeuganbieters erfüllt sind.

Teil IV – Weitere gemeinsame Bestimmungen

11 Gemeinsame Bestimmungen

Die Regelungen dieses Kapitels gelten für den Auftragnehmer dieses Fachloses. Losspezifische Regelungen im Kapitel 4 gehen vor, soweit sie weitergehende Anforderungen enthalten.

11.1 Verarbeitung von Sozial- und Gesundheitsdaten

Der Auftragnehmer verarbeitet im Rahmen dieses Fachloses grundsätzlich keine Sozial- oder Gesundheitsdaten.

Ist eine Einsichtnahme im Einzelfall unvermeidbar, erfolgt sie nur nach vorheriger Zustimmung der verantwortlichen Stelle und im erforderlichen Umfang; sie wird dokumentiert.

Soweit ausnahmsweise eine Verarbeitung im Auftrag erforderlich ist, schließt die abrufende Stelle eine eigene Vereinbarung zur Auftragsverarbeitung.

Im Übrigen gelten die Kapitel 5 bis 10 in dem dort für dieses Fachlos bestimmten Umfang.

11.2 Personalsicherheit und Vertraulichkeit

Der Auftragnehmer verpflichtet alle Personen, die Zugang zu Daten oder Systemen des Auftraggebers oder eines Bedarfsträgers erhalten, schriftlich auf die Wahrung des Sozialgeheimnisses nach § 35 SGB I sowie auf die Zweckbindungs- und Geheimhaltungspflichten nach § 78 SGB X und auf die Vertraulichkeit. Für Personen mit administrativem Zugriff oder mit Zugriff auf Sozial- und Gesundheitsdaten führt er eine Zuverlässigkeitsprüfung durch und weist diese auf Verlangen nach.

Der Auftragnehmer unterhält ein Verfahren, das bei Ausscheiden oder Aufgabenwechsel den Entzug sämtlicher Zugriffsrechte und die Rückgabe von Zugangsmitteln sicherstellt, und führt eine aktuelle Liste der Personen mit Zugriffsmöglichkeit. Die weitergehenden Anforderungen des Abschnitts 8.2 bleiben unberührt.

11.3 Arbeitsmöglichkeiten und Zugänge

Die Leistung wird grundsätzlich aus den Räumlichkeiten des Auftragnehmers erbracht. Der Auftraggeber oder, bei einem eigenen Abruf, der abrufende Bedarfsträger stellt einen gesicherten Fernzugang bereit; die Anforderungen des Abschnitts 6.3 gelten entsprechend. Arbeitsmittel sowie eingesetzte Hard- und Softwarewerkzeuge stellt der Auftragnehmer.

Vor-Ort-Termine bei der MD-IT oder bei einzelnen Bedarfsträgern sind nach Abstimmung möglich. Sie werden vorab durch die abrufende Stelle genehmigt. Reisekosten sind nicht mit dem Tagessatz oder mit der sonstigen Vergütung der Leistung abgegolten, sondern werden gesondert erstattet; erstattet werden allein die tatsächlich entstandenen Kosten einer vorab genehmigten Reise, gegen Nachweis und nur bis zu den Grenzen des Bundesreisekostengesetzes. Aufschläge, Pauschalen und

Verwaltungszuschläge werden nicht erstattet. Material- und sonstige Nebenkosten sind mit der Vergütung abgegolten. Reisezeiten werden nicht gesondert vergütet; sie werden nicht als Aufwand in Personentagen abgerechnet. An Tagen mit An- oder Abreise wird allein der tatsächlich erbrachte fachliche Leistungsaufwand abgerechnet; eine pauschale Vergütung ganzer oder halber Tagessätze findet nicht statt.

11.4 (entfallen)

Die Rechte an den Arbeitsergebnissen regeln der EVB-IT Dienstvertrag (Anlage 25.0) und die EVB-IT Dienstleistungs-AGB (Anlage 25.1).

11.5 Abgrenzung zur Rechtsberatung

Gegenstand der Leistung ist keine Rechtsberatung im Einzelfall. Mit der Prüfung rechtlicher Fragestellungen sind interne und externe juristische Berater des Auftraggebers befasst; der Auftragnehmer arbeitet mit diesen zusammen.