Leistungsbeschreibung

Version: 1.1

Datum: 03.11.2026

Vergabenummer: MD-IT KI-RV 2026

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

Anlage 03.3 — Fachlos 3: Softwarelösung zur Führung von Managementsystemen

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 8

3.2 Begriffsbestimmungen 10

Teil II – Leistung 12

4 Leistungen des Fachloses 3 12

4.1 Leistungsgegenstand des Fachloses 3 12

4.2 Funktionale Anforderungen des Fachloses 3 15

4.3 Umgang mit KI-Funktionen der Lösung 18

4.4 Betriebs- und Sicherheitsanforderungen 18

4.5 Liefergegenstände und Abnahme 19

4.6 Erprobung im Vergabeverfahren für Fachlos 3 23

4.7 Bewertungsrelevante Merkmale 24

4.8 Qualifikation des eingesetzten Personals 25

4.9 Erweiterung des Leistungsumfangs 26

Teil III – Gemeinsame Bestimmungen 28

5 Geltungsbereich der gemeinsamen Bestimmungen 28

5.1 Geltungsbereich und Schutzbedarf 28

6 Architektur, Zugriffsschutz und Trennung der Daten 29

6.1 Identitäts- und Berechtigungsmanagement 29

6.2 Verschlüsselung und Schlüsselmanagement 31

6.3 Datenhaltung, Speicherfristen und Löschung 32

6.4 Netzsicherheit und Segmentierung 33

6.5 Konfigurations- und Härtungsmanagement 34
6.6 Fernwartung und administrative Zugänge 34
6.7 Physische Sicherheit extern betriebener Komponenten 34
7 Protokollierung und Überwachung 35
7.1 Protokollierung und Beweissicherung 35
7.2 Sicherheitsbezogene Überwachung, Security Monitoring 36
8 Sicherer Betrieb, Änderungen und Resilienz 37
8.1 Test-, Schulungs- und Entwicklungsdaten 37
8.2 Personalsicherheit und Vertraulichkeit 38
8.3 Sichere Entwicklung, Schwachstellen und Lieferkette 39
8.4 Sicherheitsvorfälle 41
8.5 Verfügbarkeit, Sicherung und Notbetrieb 42
8.6 Beherrschung leistungserforderlicher technischer Abhängigkeiten 43
8.7 Störungsbearbeitung und Erreichbarkeit 44
9 Prüfrechte und Vertragsende 46
9.1 Prüfrechte, wiederkehrende Überprüfung und Betriebsdokumentation 46
9.2 Datenrückgabe, Löschung und technische Übergabe bei Vertragsende 47
10 Einsatz von Komponenten der künstlichen Intelligenz 49
10.1 Grundsätze für den Einsatz 49
Teil IV – Weitere gemeinsame Bestimmungen 52
11 Gemeinsame Bestimmungen 52
11.1 Verarbeitung von Sozial- und Gesundheitsdaten 52
11.2 Personalsicherheit und Vertraulichkeit 52
11.3 Arbeitsmöglichkeiten und Zugänge 53
11.4 Rechte an Arbeitsergebnissen 53
11.5 Abgrenzung zur Rechtsberatung 53

Teil I – Rahmen

1 Auftraggeber und Bedarfsträger

Auftraggeberin der Rahmenvereinbarung ist die MD-IT GmbH. Die nachfolgend aufgeführten Organisationen sind abrufberechtigte Bedarfsträger.

Die Grundleistung ruft der Auftraggeber mit dem Zuschlag ab. Die Lösung ist mandantenfähig; vorgesehen sind ein übergeordneter Mandant des Auftraggebers und nachgeordnete Mandanten der übrigen Bedarfsträger. Die Zugänge für den jeweiligen Mandanten ruft die Stelle ab, der dieser Mandant zugeordnet ist; mit jedem Abruf kommt ein eigener Einzelvertrag zwischen der abrufenden Stelle und dem Auftragnehmer zustande.

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 der Leistung ist die Bereitstellung und der Betrieb einer Softwarelösung, in der der Auftraggeber und die weiteren Bedarfsträger ihre Managementsysteme führen, als vom Auftragnehmer betriebener Dienst. Der Auftragnehmer betreibt, wartet und sichert die Lösung und stellt die Betriebsumgebung nach Abschnitt 5.1 Absatz 6 bereit.

Beim Einsatz von Systemen der künstlichen Intelligenz treffen den Auftraggeber und die Bedarfsträger Pflichten zu Governance, Compliance, Informationssicherheit und Datenschutz, die dokumentiert und nachgewiesen werden müssen. Die Lösung dieses Fachloses führt die hierfür erforderlichen Vorgaben, Nachweise und Auswertungen mandantenfähig; die Aufteilung der Leistungen in Fachlose regelt Kapitel 3.

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.

Für die Führung dieser Managementsysteme wird eine Softwarelösung beschafft, die der Auftragnehmer betreibt, wartet und absichert und in der die Vorgaben, Nachweise und Auswertungen mandantenfähig geführt werden. Erfasst sind die Managementsysteme für künstliche Intelligenz und für Informationssicherheit sowie die zugehörigen Anforderungen aus Governance, Compliance und Datenschutz, soweit sie in der Lösung abgebildet werden. 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 3.

Soweit zwischen den Auftragnehmern verschiedener Fachlose eine Zusammenarbeit oder ein Informationsaustausch erforderlich ist, koordiniert der Auftraggeber diesen. Abschnitt 6.4 bleibt unberührt.

Die Fachlose umfassen im Einzelnen:

Fachlos 1 umfasst die Bereitstellung und den Betrieb der KI-gestützten Lösung zur fallbezogenen Zusammenfassung als vom Auftragnehmer betriebener Dienst einschließlich Anbindung, Einführung, Schulung, Support und Pflege; maßgeblich ist die Leistungsbeschreibung des Fachloses 1.

Fachlos 2 umfasst 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 KI-Anwendungen; maßgeblich ist die Leistungsbeschreibung des Fachloses 2.

Fachlos 3 umfasst die Bereitstellung und den Betrieb einer Softwarelösung zur Führung von Managementsystemen als Cloud-Anwendung; die Betriebsumgebung stellt der Auftragnehmer nach Abschnitt 5.1 Absatz 6 bereit. Maßgeblich ist Kapitel 4.

Für Fachlos 3 wird eine Rahmenvereinbarung mit einem Unternehmen geschlossen, nämlich dem Bieter, dessen zuschlagsfähiges Angebot nach Abschluss der Angebotswertung das höchste Wertungsergebnis erzielt. Maßgeblich hierfür ist die Mandantenstruktur nach Abschnitt 4.1: Die nachgeordneten Mandanten setzen auf dem übergeordneten Mandanten des Auftraggebers auf, und zentrale Vorgaben werden aus diesem weitergegeben; das setzt eine gemeinsame Lösung voraus. Abrufberechtigt sind der Auftraggeber und die übrigen in Kapitel 1 aufgeführten Bedarfsträger. Der Auftraggeber ruft die Grundleistung mit dem Zuschlag ab. Sie umfasst den übergeordneten Mandanten nach Abschnitt 4.1, seine Grundkonfiguration, den nachgeordneten Mandanten des Auftraggebers und die weiteren nachgeordneten Mandanten, die für die Feststellung der Betriebsbereitschaft nach Abschnitt 4.5 erforderlich sind. Die übrigen Bedarfsträger rufen ihren nachgeordneten Mandanten gesondert ab; für diese weiteren Abrufe besteht keine Mindestabnahme. 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. Sämtliche Abrufe dieses Fachloses erfolgen bei diesem Rahmenvertragspartner.

Die Fachlose sind so abgegrenzt, dass die Leistung eines Fachloses ohne die der übrigen erbracht werden kann. Ergebnisse aus Fachlos 2 begründen keine über diese Leistungsbeschreibung hinausgehenden Pflichten des Auftragnehmers dieses Fachloses; eine Erweiterung des Leistungsumfangs wird nach Abschnitt 4.9 vereinbart. Sie erfolgt gegen Vergütung nach den im Vergabeverfahren festgelegten Preisen.

Mit dem Abruf einer Leistung kommt zwischen dem abrufenden Bedarfsträger und dem Auftragnehmer ein eigener Einzelvertrag zustande. Werden dabei personenbezogene Daten im Auftrag verarbeitet, schließt der abrufende Bedarfsträger einen eigenen Vertrag über die Auftragsverarbeitung nach Art. 28 der Verordnung (EU) 2016/679 in Verbindung mit § 80 des Zehnten Buches Sozialgesetzbuch. Der Vertrag über die Auftragsverarbeitung wird auf Grundlage des Musters der Anlage 29 geschlossen; Abweichungen bedürfen der Zustimmung des abrufenden Bedarfsträgers als verantwortlicher Stelle. Der Auftragnehmer hält die zugehörigen Angaben und Nachweise für jeden Bedarfsträger vor.

Wird die Lösung des Fachloses 3 eingesetzt, führt die MD-IT die Inhalte ihres Managementsystems dort; die übrigen Bedarfsträger führen die Inhalte ihres jeweiligen Mandanten. Der Auftragnehmer des Fachloses 2 erstellt die Inhalte und pflegt sie auf Verlangen des Auftraggebers und, soweit ein Bedarfsträger diese Leistungen für seinen Mandanten abruft, auf dessen Verlangen in die Lösung ein; er erhält hierfür einen auf diesen Zweck beschränkten Zugang. Der Auftragnehmer des Fachloses 3 schuldet die Verfügbarkeit und Funktionsfähigkeit der Lösung, nicht deren inhaltliche Befüllung. Kann die Lösung eine vom Auftragnehmer des Fachloses 2 vorgeschlagene Struktur nicht abbilden, entscheidet der Auftraggeber über das weitere Vorgehen; ein Anspruch auf Anpassung der Lösung entsteht dadurch nicht.

Sämtliche in die Lösung eingepflegten Inhalte verbleiben bei der MD-IT und bei dem Bedarfsträger, dessen Mandanten sie zugeordnet sind. Bei Beendigung des Vertrages gilt Abschnitt 9.2.

Ein Bieter darf für dieselbe Vergabe auf mehrere Fachlose bieten. Ergibt sich daraus ein Interessengegensatz, der die neutrale Leistungserbringung beeinträchtigen kann, insbesondere wenn derselbe Bieter sowohl die Beratungsleistung des Fachloses 2 als auch die Softwarelösung dieses Fachloses anbietet, legt er dies mit dem Angebot offen und beschreibt die Maßnahmen, mit denen er eine Beeinflussung wirksam verhindert. Gibt ein Bieter zugleich ein Angebot für Fachlos 2 ab, gilt Ziffer 11.2 der Angebotsbedingungen: Erhält er im Fachlos 2 den Zuschlag, wird sein Angebot für dieses Fachlos nicht gewertet. Im Übrigen führt das Bestehen einer solchen Beziehung für sich genommen nicht zum Ausschluss.

Soweit in dieser Leistungsbeschreibung der Auftragnehmer angesprochen wird, ist der Auftragnehmer dieses Fachloses gemeint. Das Kapitel 4 regelt die Leistung dieses Fachloses; die Kapitel 5 bis 10 gelten für sie nach Maßgabe des Kapitels 5, und das Kapitel 11 tritt hinzu.

Eine erklärte Kapazität und eine darauf bezogene Lastlogik sind für dieses Fachlos nicht vorgesehen; ein Nachweis der gleichzeitigen Leistungsfähigkeit für mehrere Bedarfsträger wird nicht verlangt.

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.

Anpassungen, die zur Einhaltung geänderter rechtlicher oder normativer Vorgaben erforderlich sind und die beauftragten Funktionen betreffen, sind im Rahmen der Pflege zu erbringen. Neue oder erweiterte funktionale Anforderungen werden gesondert beauftragt.

Soweit die Verarbeitung von Sozial- oder Gesundheitsdaten im Wege eines Cloud-Computing-Dienstes in den persönlichen Anwendungsbereich des § 393 des Fünften Buches Sozialgesetzbuch fällt, sind dessen Anforderungen einzuhalten. Ob dies für den jeweiligen Abruf zutrifft, legt der Bedarfsträger vor dem Abruf nach Kapitel 3 fest; in Betracht kommt es insbesondere für die Deutsche Rentenversicherung Knappschaft-Bahn-See als Trägerin der gesetzlichen Kranken- und Pflegeversicherung. In diesen Fällen muss die datenverarbeitende Stelle die Voraussetzungen des § 393 Absatz 2 des Fünften Buches Sozialgesetzbuch erfüllen; der Auftragnehmer benennt die datenverarbeitenden Stellen und weist deren Niederlassung im Inland nach. Ferner ist grundsätzlich ein aktuelles Testat nach dem Anforderungskatalog Cloud Computing (C5) des jeweils nach § 393 Absatz 3 und 4 des Fünften Buches Sozialgesetzbuch erforderlichen Typs vorzulegen. Die Nachweise müssen den vom Auftragnehmer erbrachten Dienst einschließlich der Anwendung und die für die Leistungserbringung eingesetzte Cloud-Infrastruktur erfassen. Zulässig ist die Kombination eines Testats des Auftragnehmers für Dienst und Anwendung mit dem Testat des Infrastrukturbetreibers; das Testat eines Betreibers der zugrunde liegenden Infrastruktur allein genügt nicht. Der Auftragnehmer benennt die im Prüfbericht enthaltenen Kriterien, die von den Bedarfsträgern umzusetzen sind. Die Übergangsregelung des § 393 Absatz 4 des Fünften Buches Sozialgesetzbuch bleibt unberührt; gleichwertige Nachweise werden nach Maßgabe der Verordnung über die Gleichwertigkeit von Nachweisen nach § 393 des Fünften Buches Sozialgesetzbuch anerkannt. Die Nachweise müssen zum Zeitpunkt der produktiven Inbetriebnahme vorliegen; mit dem Angebot sind sie vorzulegen oder, sofern das Verfahren noch nicht abgeschlossen ist, ist dessen Stand nachzuweisen. Sie sind bei Ablauf oder bei Änderung des Geltungsbereichs unaufgefordert zu aktualisieren.

Für Bedarfsträger, die nicht in den persönlichen Anwendungsbereich des § 393 des Fünften Buches Sozialgesetzbuch fallen, wird ein Testat nach dem Anforderungskatalog Cloud Computing nicht als vertragliche Mindestanforderung vorausgesetzt. Unberührt bleiben die in dieser Leistungsbeschreibung festgelegten Anforderungen an Datenschutz und Informationssicherheit. Ihre Einhaltung ist durch Nachweise auf Grundlage eines anerkannten, veröffentlichten Prüfrahmens zu belegen, insbesondere DIN EN ISO/IEC 27001, IT-Grundschutz, Anforderungskatalog Cloud Computing oder eines gleichwertigen Prüfrahmens. Die Nachweise müssen den vom Auftragnehmer erbrachten Dienst einschließlich der Anwendung und die tatsächlich genutzte Betriebsumgebung erfassen; die Kombination von Nachweisen des Auftragnehmers und des Infrastrukturdienstleisters ist zulässig, Nachweise, die sich ausschließlich auf einen Infrastrukturdienstleister beziehen, genügen nicht. Eine abgeschlossene Zertifizierung der Anwendung wird nicht vorausgesetzt; es genügen ein Prüfbericht, ein Testat oder eine gleichwertige dokumentierte Bewertung nach dem jeweiligen Prüfrahmen, sofern sie von einer Stelle erstellt ist, die vom Betrieb der bewerteten Leistung unabhängig ist. Eine Selbsteinschätzung des Auftragnehmers genügt nicht. Ist ein Verfahren bei Angebotsabgabe noch nicht

abgeschlossen, ist dessen Stand nachzuweisen; der Nachweis muss zum Zeitpunkt der produktiven Inbetriebnahme vorliegen. Für den Ort der Verarbeitung gilt Abschnitt 5.1 Absatz 6.

Die Anforderungen der beiden vorstehenden Absätze gelten, soweit in der Lösung Sozial- oder Gesundheitsdaten verarbeitet werden. Nach dem Zuschnitt dieses Fachloses ist eine solche Verarbeitung nicht vorgesehen; Abschnitt 11.1 bleibt unberührt.

Für die hier beschriebene Leistung konkretisieren das Kapitel 4 sowie die Kapitel 5 bis 10 die daraus folgenden Anforderungen. Werden die genannten Regelwerke während der Vertragslaufzeit fortgeschrieben, gilt Abschnitt 5.1 Absatz 7.

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 ist zugleich Bedarfsträgerin und Empfängerin der Leistungen dieses Fachloses.

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 Organisationen.

Abrufende Stelle ist der Auftraggeber für die Grundleistung und seinen übergeordneten Mandanten sowie der jeweilige Bedarfsträger für seinen nachgeordneten Mandanten; sie ist Partei des jeweiligen Einzelvertrags.

Mandant bezeichnet den in der Lösung getrennt geführten Bereich einer Stelle. Vorgesehen sind ein übergeordneter Mandant des Auftraggebers und nachgeordnete Mandanten der übrigen Bedarfsträger nach Abschnitt 4.1.

Managementsystem bezeichnet das in der Lösung geführte System zur Steuerung und zum Nachweis der Anforderungen, insbesondere für künstliche Intelligenz und für Informationssicherheit, einschließlich seiner Vorgaben, Nachweise, Register, Dokumente und Auswertungen.

Lösung bezeichnet die vom Auftragnehmer bereitgestellte Software zur Führung der Managementsysteme einschließlich ihres Betriebs.

Komponente der künstlichen Intelligenz bezeichnet einen Bestandteil der Lösung, der auf Verfahren der künstlichen Intelligenz beruht, insbesondere Sprachmodelle sowie die zugehörigen Verfahren zur Auswahl und Aufbereitung von Quellen; solche Funktionen werden nur nach Abschnitt 4.3 eingesetzt.

Leistungserforderliche technische Abhängigkeit bezeichnet technische Komponenten, Dienste, Konfigurationen, Vertrauensstellungen, Berechtigungen, Kontingente und sonstige technische

Voraussetzungen, deren Ablauf, Ausfall, Änderung, Widerruf oder Wegfall die Verfügbarkeit, Integrität oder Vertraulichkeit der vertragsgegenständlichen Leistung beeinträchtigen kann. Hierzu zählen insbesondere kryptografisches Material, externe Dienste und Schnittstellen, Identitäts- und Authentisierungsdienste, Lizenzen, Kontingente und Zugangsmerkmale.

Kryptografisches Material bezeichnet Zertifikate, öffentliche und private Schlüssel, Signatur- und Vertrauensanker sowie vergleichbares Material, das bei der Erbringung der vertragsgegenständlichen Leistung eingesetzt wird. Leistungserforderlich ist kryptografisches Material, das eine leistungserforderliche technische Abhängigkeit darstellt. Schnittstellenrelevant ist der Teil des leistungserforderlichen kryptografischen Materials, der an Schnittstellen zum Auftraggeber oder zu den Bedarfsträgern eingesetzt oder vom Auftraggeber bereitgestellt oder konfiguriert wird. Nachweise über Zertifizierungen, Testate und sonstige Sicherheitsprüfungen der Betriebsumgebung sind kein kryptografisches Material im Sinne dieser Bestimmung.

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 den Regelungen dieses Fachloses bleibt unberührt.

Teil II – Leistung

4 Leistungen des Fachloses 3

4.1 Leistungsgegenstand des Fachloses 3

Gegenstand des Fachloses 3 ist die Bereitstellung und der Betrieb einer Softwarelösung, in der der Auftraggeber und die weiteren Bedarfsträger ihre Managementsysteme führen. Die Leistung wird ausschließlich als Cloud-Anwendung erbracht, die der Auftragnehmer oder ein von ihm beauftragter Dienstleister betreibt. Eine Überlassung von Software zum Betrieb durch den Auftraggeber oder einen Bedarfsträger und ein Betrieb in deren Räumlichkeiten oder Infrastruktur sind nicht Gegenstand der Leistung. Die Betriebsumgebung stellt der Auftragnehmer nach Abschnitt 5.1 Absatz 6 bereit; maßgeblich ist, dass Betrieb, Wartung und Absicherung beim Auftragnehmer verbleiben.

Die Lösung bildet die Anforderungen der Norm DIN EN ISO/IEC 42001 einschließlich der Maßnahmen des Anhangs A ab und ermöglicht daneben die Führung von Managementsystemen für Informationssicherheit nach der Norm DIN EN ISO/IEC 27001 sowie nach der IT-Grundschutz-Methodik des Bundesamts für Sicherheit in der Informationstechnik einschließlich des Notfallmanagements. Ebenso ermöglicht sie die Führung eines Managementsystems für den Schutz personenbezogener Daten nach der Norm DIN EN ISO/IEC 27701 sowie die Erfassung und Nachverfolgung der Pflichten aus der Verordnung (EU) 2024/1689, insbesondere der Einordnung eingesetzter Systeme der künstlichen Intelligenz, der zugehörigen Nachweise und der Fristen. Ebenso bildet sie die Anforderungen des Branchenspezifischen Sicherheitsstandards für die gesetzliche Kranken- und Pflegeversicherung nach § 393 Absatz 5 Nummer 3 in Verbindung mit § 392 des Fünften Buches Sozialgesetzbuch ab. Dieser Katalog gehört zum verbindlich mitzuliefernden Katalogset; der Auftragnehmer pflegt ihn über die Vertragslaufzeit und schreibt ihn bei Änderungen fort. Für den Nachweis der hierfür erforderlichen Nutzungs- und Weitergaberechte gilt die Nachweispflicht für die Inhalte der IT-Grundschutz-Methodik in diesem Abschnitt entsprechend.

Weitere Anforderungskataloge, Normen und eigene Vorgaben des Auftraggebers oder eines Bedarfsträgers können aufgenommen, gepflegt und den vorhandenen Inhalten gleichgestellt werden; dies ist durch die Administration des jeweiligen Mandanten ohne Mitwirkung des Auftragnehmers und ohne gesonderte Vergütung möglich.

In Betracht kommen insbesondere der BSI-Standard 200-4 oder die Norm ISO 22301 für das Notfallmanagement, die Norm DIN EN ISO 9001 für das Qualitätsmanagement, die Anforderungen an barrierefreie Informationstechnik, weitere branchenspezifische Sicherheitsstandards, soweit sie für einen Bedarfsträger einschlägig sind, sowie die Pflichten aus dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und der hierzu ergangenen Rechtsverordnung, soweit ein Bedarfsträger Betreiber einer kritischen Anlage ist. Der Auftragnehmer beschreibt mit dem Angebot, in welcher Form eigene Kataloge angelegt und Anforderungen verschiedener Regelwerke einander zugeordnet werden können. Ist ein Bedarfsträger Betreiber einer kritischen Anlage und sind die in der Lösung geführten Managementsysteme für deren Funktionsfähigkeit maßgeblich, bildet die Lösung auch die hierfür geltenden Anforderungen und Nachweise ab.

Die vorstehenden Funktionen und Anforderungskataloge gehören zum Mindestumfang jedes nach Kapitel 3 abgerufenen Mandanten; für einen zusätzlich abrufenden Bedarfsträger dürfen sie weder funktional eingeschränkt noch gesondert vergütet werden. Die Grundleistung wird nach Maßgabe des Kapitels 3 mit dem Zuschlag abgerufen. Die weiteren Leistungen werden auf Abruf erbracht; für sie wird keine Mindestabnahme vereinbart. 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.

Der Bieter weist nach, dass er für die vertragsgemäße Bereitstellung, Integration, Aktualisierung und Nutzung der in der Lösung enthaltenen Inhalte der IT-Grundschutz-Methodik über sämtliche erforderlichen Nutzungs-, Lizenz- und Weitergaberechte verfügt. Eine unmittelbare Lizenzvereinbarung mit dem Bundesamt für Sicherheit in der Informationstechnik kann als Nachweis dienen; gleichwertige rechtliche Berechtigungen werden anerkannt, sofern sie die vollständige und während der Vertragslaufzeit aktualisierbare Bereitstellung der geschuldeten Inhalte gewährleisten. Der Nachweis ist mit dem Angebot vorzulegen.

Die Lösung ist mandantenfähig. Vorgesehen ist eine Struktur aus einem übergeordneten Mandanten des Auftraggebers und nachgeordneten Mandanten der Organisationen. Der Auftraggeber führt neben dem übergeordneten Mandanten einen eigenen nachgeordneten Mandanten, in dem er sein eigenes Managementsystem führt; der übergeordnete Mandant dient allein den gemeinsamen Vorgaben und der aggregierten Auswertung. Im übergeordneten Mandanten werden gemeinsame Vorgaben, Richtlinien, Maßnahmen und Vorlagen gepflegt und den nachgeordneten Mandanten bereitgestellt. Dabei ist zu unterscheiden zwischen Inhalten, die verbindlich zu übernehmen und im nachgeordneten Mandanten nicht veränderbar sind, und Vorlagen, die organisationsbezogen angepasst werden dürfen. Änderungen im übergeordneten Mandanten werden nachvollziehbar an die nachgeordneten Mandanten weitergegeben; der Zeitpunkt der Übernahme ist erkennbar. Jede Organisation führt ihr Managementsystem im Übrigen eigenständig; ein Zugriff auf Inhalte anderer Organisationen findet nicht statt. Maßgeblich ist das in diesem Absatz beschriebene Ergebnis, nicht die technische Umsetzung oder deren Bezeichnung. Eine Lösung erfüllt diesen Absatz auch dann, wenn sie die Trennung der Inhalte und die Weitergabe zentraler Vorgaben auf anderem Weg als über getrennte Mandanteninstanzen herstellt, sofern die Trennung technisch durchgesetzt wird, jede Organisation ihre Rollen und Berechtigungen eigenständig vergibt und die Prüffälle F-01 und F-02 nach Abschnitt 4.5 erfüllt werden.

Der Auftraggeber kann den Umsetzungsstand der nachgeordneten Mandanten in aggregierter Form auswerten. Ein Zugriff auf Inhalte einzelner Mandanten findet dabei nicht statt; die Auswertung beschränkt sich auf Kennzahlen, die keine Rückschlüsse auf einzelne Feststellungen zulassen.

Für die Auslegung und die Angebotskalkulation gilt folgendes Mengengerüst. Angegeben sind Maximalwerte über alle Organisationen; sie begründen keine Mindestabnahme. Vorzusehen sind ein übergeordneter Mandant des Auftraggebers und bis zu 18 nachgeordnete Mandanten, nämlich je einer für jede der in Kapitel 1 aufgeführten Stellen einschließlich des Auftraggebers. Für die Dimensionierung ist von anfänglich 20 Zugängen auszugehen. Die Lösung unterscheidet Zugänge nach dem Umfang der Berechtigung: bearbeitende Zugänge, die Inhalte erstellen und ändern; freigebende Zugänge, die Inhalte prüfen und in Kraft setzen; administrative Zugänge, die Mandanten, Rollen, Berechtigungen und Konfiguration verwalten; sowie lesende Zugänge, die Inhalte einsehen, Schulungsinhalte abrufen und deren Kenntnisnahme bestätigen. Für administrative Zugänge gelten ergänzend die Anforderungen des Abschnitts 6.6.

Für die Kalkulation ist von folgenden Zugangsmengen auszugehen: bis zu 300 bearbeitende Zugänge, bis zu 100 freigebende Zugänge, bis zu 100 administrative Zugänge sowie lesende Zugänge für sämtliche Beschäftigten der Bedarfsträger; hierfür ist von 15.000 Zugängen auszugehen. Dieser Wert ist Auslegungsgröße; die in Kapitel 1 genannte Zahl der Beschäftigten liegt darunter.

Diese Mengen sind Kapazität der Grundleistung, mit ihr vollständig zu kalkulieren und stehen der Gesamtheit der Bedarfsträger zur Verfügung; der Auftraggeber beschafft sie mit der Grundleistung für alle abrufberechtigten Stellen. Sie werden nicht auf die nachgeordneten Mandanten aufgeteilt, und ein später abrufender Bedarfsträger mindert nicht die dem Auftraggeber zur Verfügung stehende Kapazität.

Ruft ein Bedarfsträger nach Kapitel 3 einen eigenen nachgeordneten Mandanten ab, so gilt hierfür ein einheitlicher Preis je Mandant, unabhängig von der Größe der abrufenden Stelle und von der Zahl der dort benötigten Zugänge; die in diesem Mandanten eingerichteten Zugänge zählen gegen die vorstehende Kapazität der Grundleistung, und eine gesonderte Vergütung je Zugang findet insoweit nicht statt. Der Bieter weist im Preisblatt aus, wie sich die Vergütung auf die Zugangsarten verteilt, ob lesende Zugänge gesondert vergütet werden und zu welchen Preisen Zugänge oberhalb der vorstehenden Mengen abgerufen werden können. Der Bedarf je Mandant ist unterschiedlich, weil einzelne Bedarfsträger weitere eigene Managementsysteme in der Lösung führen können; der einheitliche Preis je Mandant bleibt davon unberührt.

Für produktbezogene Beratungs- und Unterstützungsleistungen sowie für Entwicklungsleistungen zur Anpassung der Standardkonfigurationen beträgt die Höchstabrufmenge insgesamt 500 Personentage je Vertragsjahr der Rahmenvereinbarung über alle Bedarfsträger; die abrufende Stelle bestimmt je Abruf, welche Leistungsart benötigt wird. Auf diese Menge werden ferner Schulungsleistungen angerechnet, die über die Einweisung nach Abschnitt 4.5 Absatz 2 hinausgehen. Reisezeiten werden nach Abschnitt 11.3 Absatz 2 nicht vergütet und nicht angerechnet. Die Leistungen werden auf Abruf erbracht; eine Zusage über ihren Umfang besteht nicht.

Produktbezogen sind Leistungen zu Einrichtung, Konfiguration und Nutzung der Lösung; die methodische Beratung zum Aufbau und Betrieb der Managementsysteme ist Gegenstand des Fachloses 2. Anpassungen erfolgen innerhalb der Konfigurations- und Erweiterungsmöglichkeiten der Standardlösung; Änderungen am Produktkern sind nicht Gegenstand dieser Abrufleistungen. Unberührt bleibt die Herstellung des nach Kapitel 4 geschuldeten Leistungsumfangs. Stellt ein Bieter einzelne der dort geforderten Funktionen erst durch Anpassung oder Weiterentwicklung seiner Lösung her, so ist das zulässig; diese Leistung ist mit der Vergütung der Lösung abgegolten, wird nicht auf die vorstehende Höchstabrufmenge angerechnet und begründet keinen Anspruch auf gesonderte Vergütung.

Anpassungen bleiben bei Aktualisierungen der Lösung erhalten oder werden vom Auftragnehmer ohne gesonderte Vergütung übertragen; sie werden dokumentiert und bei Beendigung nach Abschnitt 9.2 übergeben. Der Bieter weist im Preisblatt Tagessätze je Leistungsart und Qualifikationsprofil nach Abschnitt 4.8 aus. Für die Abrechnung dieser Leistungen gelten die im Vergabeverfahren festgelegten Preise und Tagessätze. Die Mengen dienen der Angebotswertung und der Auftragswertschätzung; sie begründen keine Mindestabnahme.

4.2 Funktionale Anforderungen des Fachloses 3

Die Lösung stellt mindestens die nachstehenden Funktionen bereit: Verzeichnis der Managementsystem-Gegenstände einschließlich der eingesetzten Systeme der künstlichen Intelligenz, Zuordnung von Anforderungen zu Maßnahmen und Nachweisen, Risikobeurteilung mit Risikoregister, Maßnahmenverfolgung, Dokumentenlenkung mit Versionierung und Freigabe, Auditplanung und Auditdurchführung, Managementbewertung sowie Auswertungen und Berichte. Vorzusehen ist eine dokumentierte Schnittstelle zur Dokumentationsplattform des Auftraggebers.

Ein einmal hinterlegter Nachweis kann mehreren Anforderungen aus unterschiedlichen Regelwerken zugeordnet werden, sodass er nicht mehrfach zu erbringen ist. Die Zuordnung ist nachvollziehbar und kann vom Auftraggeber und von den Bedarfsträgern in ihrem jeweiligen Mandanten gepflegt werden. Weitere Regelwerke können aufgenommen werden, ohne dass die bestehenden Zuordnungen neu erstellt werden müssen.

Mit der Lösung werden mindestens Anforderungskataloge zu den nachstehenden Regelwerken mitgeliefert: DIN EN ISO/IEC 27001 einschließlich Anhang A, DIN EN ISO/IEC 42001 einschließlich Anhang A, DIN EN ISO/IEC 27701 sowie die IT-Grundschutz-Methodik des Bundesamtes für Sicherheit in der Informationstechnik einschließlich des Standards zum Notfallmanagement. Der Auftragnehmer hält diese Kataloge auf dem jeweils geltenden Stand. Eine Neufassung, die einzelne Anforderungen ändert, bildet er innerhalb von sechs Monaten nach ihrer Veröffentlichung ab; eine vollständige Neufassung eines Regelwerks oder einen Wechsel seiner Methodik innerhalb von zwölf Monaten. Im zweiten Fall legt er innerhalb von drei Monaten nach der Veröffentlichung einen Umsetzungsplan mit Zwischenständen vor und setzt ihn um. Bestehende Zuordnungen bleiben dabei erhalten, und betroffene übernommene Inhalte werden mit ihrer Herkunft ausgewiesen. Die Mitlieferung und die Fortschreibung sind in der Vergütung enthalten. Weitere Kataloge, die der Bieter mitliefert, benennt er im Angebot; werden sie gesondert vergütet, weist er dies im Preisblatt aus.

Der Auftraggeber und die Bedarfsträger können in ihrem jeweiligen Mandanten eigene Anforderungskataloge und Bausteine selbst anlegen, ändern und in Betrieb nehmen, ohne dass hierfür eine Leistung des Auftragnehmers erforderlich ist. Ein Baustein umfasst mindestens Bezeichnung, Kennung, Zielsetzung, die zugehörigen Anforderungen mit eigener Kennung, Text und Verbindlichkeitsstufe sowie die Angabe, auf welche Arten von Werten oder Prozessen er anzuwenden ist. Bausteine und Kataloge können versioniert, in Entwurfsfassungen vorgehalten, freigegeben und außer Kraft gesetzt werden; frühere Fassungen bleiben nachvollziehbar.

Selbst angelegte Bausteine und Kataloge stehen den mitgelieferten in vollem Umfang gleich. Sie können insbesondere Werten, Prozessen, Maßnahmen, Nachweisen und Risiken zugeordnet, in die Modellierung und in die Ermittlung des Umsetzungsstands einbezogen, in die Mehrfachzuordnung von Nachweisen aufgenommen und in Auswertungen sowie Auditplanungen verwendet werden.

Bausteine und einzelne Anforderungen aus mitgelieferten oder bereits vorhandenen Katalogen können in eigene Kataloge übernommen und dort angepasst werden. Bei einer Übernahme bleibt die Herkunft erkennbar; Abweichungen gegenüber der Ursprungsfassung sind nachvollziehbar. Wird der Ursprungskatalog fortgeschrieben, weist die Lösung die betroffenen übernommenen Inhalte aus.

In gleicher Weise können der Auftraggeber und die Bedarfsträger in ihrem jeweiligen Mandanten eigene Maßnahmen und Maßnahmenkataloge anlegen und pflegen sowie mitgelieferte Maßnahmen anpassen. Maßnahmen können mehreren Anforderungen aus verschiedenen Katalogen zugeordnet und mit Verantwortlichkeit, Fälligkeit, Umsetzungsstand und Nachweisen versehen werden.

Der Auftraggeber kann die Bewertungsmaßstäbe selbst festlegen; die Bedarfsträger können dies für ihren Mandanten, soweit der übergeordnete Mandant sie nicht nach Abschnitt 4.1 als verbindlich zu übernehmende Vorgabe festgelegt hat. Dies umfasst mindestens die Kategorien und Definitionen des Schutzbedarfs, die Skalen für Eintrittswahrscheinlichkeit und Schadenshöhe einschließlich der daraus abgeleiteten Risikoklassen und Schwellenwerte, die Kriterien für die Annahme verbleibender Risiken sowie ein mehrstufiges Modell zur Bewertung von Reife- und Umsetzungsgraden mit eigenen Stufendefinitionen.

Ferner können eigene Klassifizierungsschemata, Objektarten mit zusätzlichen Feldern, Freigabe- und Bearbeitungsabläufe sowie Vorlagen für Dokumente und Berichte angelegt und geändert werden. Änderungen an diesen Festlegungen wirken sich nicht rückwirkend auf bereits abgeschlossene Bewertungen aus; frühere Fassungen bleiben nachvollziehbar.

Kataloge können über eine dokumentierte Schnittstelle oder in einem offenen, strukturierten Dateiformat eingespielt und ausgeleitet werden. Der Auftragnehmer beschreibt Format und Verfahren. Die eingespielten Inhalte verbleiben beim Auftraggeber und bei dem Bedarfsträger, dessen Mandanten sie zugeordnet sind; Abschnitt 4.5 bleibt unberührt.

Die Lösung sieht ein Rollenkonzept vor, das mindestens zwischen zentraler Administration beim Auftraggeber, Administration je Mandant, Bearbeitung und lesendem Zugriff für Prüfende unterscheidet. Rollen und Berechtigungen werden je Mandant eigenständig vergeben. Ein lesender Zugriff für interne und externe Prüfende ist ohne Änderungsrechte möglich und zeitlich befristbar.

Die Anmeldung kann über die Identitätsverwaltung der jeweiligen Organisation erfolgen; die Lösung unterstützt hierfür verbreitete, offene Verfahren zur föderierten Anmeldung. Für Zugänge mit erweiterten Rechten ist eine Mehrfaktor-Authentifizierung verpflichtend.

Innerhalb eines Mandanten lassen sich Organisationseinheiten, Standorte und Prozesse abbilden und einem Geltungsbereich zuordnen. Die Struktur ist nachträglich änderbar, ohne dass bestehende Zuordnungen verlorengehen.

Das Verzeichnis erfasst klassische Werte der Informationsverarbeitung und Systeme der künstlichen Intelligenz gemeinsam und erlaubt deren Verknüpfung mit Prozessen, Risiken, Maßnahmen und Nachweisen.

Bestehende Inhalte können übernommen werden. Der Auftragnehmer beschreibt, in welchen Formaten und in welchem Umfang eine Übernahme aus anderen Lösungen möglich ist, und benennt die Grenzen des Verfahrens. Bei automatisierten Übernahmen und Abgleichen sind Ausführungsstatus, Zeitpunkt, verarbeiteter Umfang und aufgetretene Fehler nachvollziehbar; fehlgeschlagene Übertragungen können kontrolliert wiederholt werden.

Maßnahmen und Aufgaben können Personen zugewiesen und mit Fälligkeiten versehen werden. Die Lösung erinnert an offene und überfällige Aufgaben und weist den Bearbeitungsstand aus.

Änderungen an Bewertungen, Maßnahmen, Nachweisen und Dokumenten werden mit Zeitpunkt und handelnder Person nachvollziehbar aufgezeichnet. Die Aufzeichnung ist auswertbar und für Prüfungen verwendbar.

Das Preisblatt gibt die Bezugsgröße der Vergütung verbindlich vor, damit die Angebote vergleichbar sind. Anzugeben ist ein Gesamtpreis je Jahr für den Leistungsumfang des Mengengerüsts nach Abschnitt 4.1, aufgegliedert nach den dort genannten Zugangsarten. Der Bieter stellt zusätzlich sein eigenes Lizenz- und Abrechnungsmodell und dessen Bezugsgröße dar, insbesondere ob nach Mandanten, benannten oder gleichzeitigen Nutzern, nach Organisations- oder Projektgröße oder pauschal abgerechnet wird, und erläutert, wie er es auf die Bezugsgröße des Preisblatts umgerechnet hat. Ein abweichend aufgebautes Modell führt nicht zum Ausschluss, solange die Umrechnung nachvollziehbar ist. Einzelheiten regelt das Preisblatt. Die Preise für Bereitstellung und Betrieb bleiben bis zum Wirksamwerden der ersten Anpassung zum 1. April 2029 unverändert. Die erste Anpassung erfasst ausschließlich die Indexentwicklung zwischen den Jahresdurchschnitten 2027 und 2028; Indexentwicklungen bis einschließlich 2027 sind einzukalkulieren. Für die restliche Vertragslaufzeit sieht der Vertrag eine Anpassungsregelung vor, die sich an einer veröffentlichten Indexreihe des Statistischen Bundesamtes orientiert, Anpassungen nach oben und nach unten in gleicher Weise zulässt, einmal je Kalenderjahr zum 1. April, frühestens zum 1. April 2029, wirkt und je Anpassungsschritt auf drei vom Hundert begrenzt ist; sie erfasst allein den im Preisblatt getrennt ausgewiesenen Anteil für den laufenden Betrieb der Verarbeitungsinfrastruktur, während die übrigen Preisbestandteile über die Laufzeit fest bleiben. Einzelheiten, insbesondere die maßgebliche Indexreihe, der maßgebliche Erhebungszeitraum, ein Schwellenwert und das Verfahren bei Umstellung des Basisjahres oder Wegfall der Reihe, regelt der Vertrag.

Geschäftsprozesse können erfasst, kategorisiert und mit den Werten der Informationsverarbeitung verknüpft werden. Der Schutzbedarf wird je Prozess festgelegt und auf die zugeordneten Werte vererbt; bei mehreren zusammenlaufenden Abhängigkeiten wird er nachvollziehbar ermittelt und kann begründet abweichend festgelegt werden.

Externe Dienstleister können erfasst, einzelnen Prozessen zugeordnet und mit den wesentlichen Angaben ihrer Verträge hinterlegt werden, insbesondere Laufzeit, Leistungsumfang und vereinbarte Dienstgüte. Sie können Gegenstand strukturierter und wiederkehrender Bewertungen sein; Erhebungen, Nachweise, festgestellte Risiken und daraus abgeleitete Maßnahmen bleiben dem jeweiligen Dienstleister zugeordnet.

Für die Risikobeurteilung stehen vorbelegte Kataloge zu Gefährdungen, Bedrohungen und Schwachstellen sowie Prüflisten zur Ermittlung des Umsetzungsstands zur Verfügung; sie sind organisationsbezogen anpassbar. Risiken können nach Behandlung erneut bewertet werden; die Annahme verbleibender Risiken und die Zulassung von Ausnahmen werden mit Begründung, Verantwortlichkeit und Geltungsdauer dokumentiert.

Das Notfallmanagement wird in derselben Lösung geführt. Es umfasst die Ermittlung kritischer Prozesse und ihrer Abhängigkeiten, Auswirkungsanalysen, die Festlegung von Wiederanlauf- und Wiederherstellungszielen, Notfall- und Wiederanlaufpläne mit den zugehörigen Verantwortlichkeiten sowie die Planung und Dokumentation von Übungen und eingetretenen Notfällen. Das Notfallmanagement

nach diesem Absatz und die Erfassung und Bewertung externer Dienstleister sind Bestandteil der geschuldeten Leistung. Werden diese Funktionen beim Bieter als eigenständige Module geführt, sind sie im Gesamtpreis nach Abschnitt 4.2 enthalten und im Preisblatt gesondert auszuweisen.

Inhalte können revisionssicher archiviert und danach unveränderbar aufbewahrt werden. Gesetzliche Löschungs- und Berichtigungspflichten bleiben unberührt; die Lösung ermöglicht die Löschung archivierter Inhalte auf Weisung der für die Verarbeitung verantwortlichen Stelle unter Protokollierung des Vorgangs.

Auswertungen stehen als Übersichtsseite mit verdichteter Darstellung sowie als Bericht zur Verfügung; Such-, Filter- und Sortierfunktionen sind vorhanden. Für die Ersterfassung größerer Bestände stehen Funktionen zur Übernahme und Vervielfältigung von Datensätzen bereit.

Strukturierte Erhebungen können erstellt und an Personen innerhalb und außerhalb der Lösung übermittelt werden. Die Beantwortung erfolgt über einen geschützten Zugang; die Antworten werden dem jeweiligen Objekt zugeordnet. Für wiederkehrende Bewertungen, einschließlich der Einordnung von Systemen der künstlichen Intelligenz nach der KI-Verordnung, können Vorlagen hinterlegt werden.

4.3 Umgang mit KI-Funktionen der Lösung

Enthält die Lösung Funktionen, die auf Verfahren der künstlichen Intelligenz beruhen, sind sie je Mandant durch die Administration dieses Mandanten ohne Mitwirkung des Auftragnehmers abschaltbar; im Auslieferungszustand sind sie deaktiviert. Über ihre Nutzung entscheidet die Stelle, die den jeweiligen Mandanten führt. Inhalte des Managementsystems, insbesondere Risikobeurteilungen, Auditfeststellungen und Schwachstellen, werden nicht ohne gesonderte Zustimmung an Verfahren der künstlichen Intelligenz übergeben. Von solchen Funktionen erzeugte Vorschläge sind als solche erkennbar und werden nicht als geprüfte Feststellungen ausgegeben. Eine Nutzung der Inhalte zu Trainings- oder Weiterentwicklungszwecken ist ausgeschlossen. Der Auftragnehmer benennt die eingesetzten Funktionen, die dabei verarbeiteten Daten und die Verarbeitungsstandorte. Von diesen Funktionen erzeugte Vorschläge werden nicht ohne eine gesonderte Handlung einer berechtigten Person als Feststellung, Bewertung, Maßnahme oder sonstige inhaltliche Änderung in das Managementsystem übernommen. Das gilt auch für Funktionen, die über das Erzeugen von Vorschlägen hinaus selbst Schritte ausführen; sie ändern Inhalte des Managementsystems nicht selbständig. Ausgeführte Schritte werden protokolliert, sind dem jeweiligen Mandanten zuzuordnen und für dessen Administration einsehbar. Inhalte des Managementsystems werden nur mit gesonderter Zustimmung der den Mandanten führenden Stelle an Dienste außerhalb der Lösung übermittelt; das gilt auch für Aufforderungen an Beschäftigte zur Mitwirkung und für die dabei mitgeteilten Angaben. Der Auftragnehmer benennt die hierfür genutzten Dienste, die Empfängerkreise und die übermittelten Datenarten. Die Übermittlung ist je Mandant durch die Administration dieses Mandanten abschaltbar und im Auslieferungszustand deaktiviert.

4.4 Betriebs- und Sicherheitsanforderungen

Für Fachlos 3 gelten die Kapitel 5 bis 10 entsprechend; maßgeblich sind die dortigen Anforderungen an einen vom Auftragnehmer betriebenen Dienst, insbesondere zu Architektur und Zugriffsschutz, Mandantentrennung, Verschlüsselung und Schlüsselverwaltung, Datenhaltung und Löschung,

Protokollierung, sicherem Betrieb, Sicherheitsvorfällen, Verfügbarkeit, Prüfrechten und Vertragsende. Die Verarbeitung erfolgt ausschließlich innerhalb des Europäischen Wirtschaftsraums.

Es gelten die Anforderungen an Verfügbarkeit und Notbetrieb nach Abschnitt 8.5, an die Beherrschung leistungserforderlicher technischer Abhängigkeiten nach Abschnitt 8.6 sowie an Störungsbearbeitung und Erreichbarkeit nach Abschnitt 8.7. Der Auftragnehmer stellt Aktualisierungen einschließlich sicherheitsrelevanter Korrekturen bereit und spielt sie ein; sie sind in der Vergütung enthalten.

4.5 Liefergegenstände und Abnahme

Mit dem Angebot vorzulegen sind: eine Beschreibung der Mandantenstruktur und der Übernahmemechanismen, eine Darstellung der abgebildeten Regelwerke und der Zuordnung von Nachweisen, ein Einführungs- und Schulungskonzept sowie eine Angabe, welche der nach Kapitel 4 geforderten Funktionen in der angebotenen Lösung vorhanden sind und welche der Bieter erst herstellt, jeweils mit dem Zeitpunkt ihrer Bereitstellung; für jede erst herzustellende Funktion ein Umsetzungskonzept, das den Lösungsweg, Meilensteine mit Zwischenständen, die Verantwortlichkeiten sowie die hierfür benötigten Mitwirkungsleistungen des Auftraggebers und der Bedarfsträger benennt. Ferner vorzulegen ist die vollständig ausgefüllte Anforderungserfüllungsmatrix nach der Anlage 11.3. Zertifikate und Prüfnachweise für die genutzte Betriebsumgebung, über die der Bieter verfügt, sind nicht mit dem Angebot, sondern auf Anforderung des Auftraggebers vor Zuschlag innerhalb der von ihm gesetzten Frist vorzulegen (Ziffer 12.1 der Angebotsbedingungen). Weil im Fachlos 3 nach Abschnitt 3.1 keine Sozial- oder Gesundheitsdaten verarbeitet werden, sind die dort genannten Testate und Nachweise nach § 393 des Fünften Buches Sozialgesetzbuch und nach einem anerkannten Prüfrahmen nicht Voraussetzung des Zuschlags; ihr Fehlen führt nicht zum Ausschluss.

Zur Herbeiführung der Betriebsbereitschaft erbringt der Auftragnehmer die Einrichtung der Mandanten, die Konfiguration nach den Vorgaben des Auftraggebers und, für den nachgeordneten Mandanten eines Bedarfsträgers, nach dessen Vorgaben, die Übernahme vorhandener Inhalte im vereinbarten Umfang sowie die Einweisung der benannten Schlüsselnutzer. Die Einweisung erfolgt über Videokonferenz oder vor Ort; Schulungsunterlagen werden zusätzlich in digitaler Form überlassen.

Der Auftraggeber ruft die Grundleistung mit dem Zuschlag ab. Sie ist innerhalb von sechs Wochen nach Abruf produktiv bereitzustellen, innerhalb von zwei Wochen nach Abruf, wenn ein aktueller Bericht einer unabhängigen Sicherheitsprüfung des Standardstands der angebotenen Lösung nach Abschnitt 8.3 Absatz 6 vorliegt.

Zur produktiven Bereitstellung gehören der übergeordnete Mandant des Auftraggebers, seine Grundkonfiguration, die Anbindung an die Identitätsverwaltung des Auftraggebers sowie mindestens zwei nachgeordnete Mandanten, darunter der nachgeordnete Mandant des Auftraggebers, an denen die Übernahmemechanismen und die aggregierte Auswertung nach den Prüffällen F-01 und F-02 festgestellt werden können.

Für den einzelnen Bedarfsträger werden der nachgeordnete Mandant eingerichtet, die Anbindung an seine Identitätsverwaltung hergestellt, die Konfiguration vorgenommen und die Einweisung erbracht, sobald er abruft; hierfür gilt dieselbe Frist ab seinem Abruf. Wird die Umgebung nach Abschnitt 4.6 in den Wirkbetrieb überführt, gilt dieselbe Frist ab Zuschlag.

Funktionen, die der Bieter nach seiner Angabe zum Angebot erst herstellt, sind abweichend hiervon zu dem von ihm benannten Zeitpunkt bereitzustellen, spätestens jedoch sechsundzwanzig Wochen nach Zuschlag; bis dahin wird die Lösung mit den vorhandenen Funktionen betrieben.

Der vom Bieter benannte Zeitpunkt ist verbindlich und wird Vertragsbestandteil. Der Zeitpunkt geht nach Maßgabe des Wertungsmerkmals W-09 in die Angebotswertung ein. Das mit dem Angebot vorzulegende Umsetzungskonzept wird ebenfalls Vertragsbestandteil. Die auf eine erst herzustellende Funktion bezogenen funktionalen Abnahmekriterien dieses Abschnitts werden zu dem benannten Zeitpunkt nachgeholt; ihr Ergebnis wird dokumentiert. Bezeichnet der Bieter eine Funktion als vorhanden, so schuldet er sie zur Feststellung der Betriebsbereitschaft; die vorstehende Frist gilt für sie nicht. Aufwand und Risiko der Herstellung liegen beim Auftragnehmer.

Die Betriebsbereitschaft wird gemeinsam festgestellt. Geprüft werden die Einrichtung der zur Grundleistung gehörenden Mandanten, die Wirksamkeit der Übernahmemechanismen zwischen übergeordnetem und nachgeordneten Mandanten, die Anmeldung über die Identitätsverwaltung des Auftraggebers sowie die in Abschnitt 4.2 genannten Funktionen. Für jeden weiteren Bedarfsträger werden die Einrichtung seines Mandanten und die Anmeldung über seine Identitätsverwaltung mit seinem Abruf gesondert festgestellt. Die Feststellung der Betriebsbereitschaft setzt voraus, dass die Prüffälle F-01 bis F-03 erfüllt sind. Funktionen, die der Bieter erst zu dem von ihm benannten Zeitpunkt bereitstellt, werden zu diesem Zeitpunkt gesondert geprüft und abgenommen; bis dahin gilt die Betriebsbereitschaft insoweit als nicht festgestellt. Betrifft eine solche Funktion einen der Prüffälle F-01 bis F-03, so wird die Betriebsbereitschaft für die übrigen Leistungsteile festgestellt und für diesen Prüffall mit dessen Abnahme nachgeholt; Satz 4 steht dem nicht entgegen. Weitere Einzelheiten werden im Vergabeverfahren festgelegt.

Zur Prüfung der Datenportabilität wird mit einem repräsentativen Testbestand die Übernahme vorhandener Inhalte sowie deren anschließende Ausleitung nach den Anforderungen des Abschnitts 9.2 geprüft. Nachzuweisen ist, dass die fachliche Struktur und die für eine Weiterverarbeitung erforderlichen Beziehungen und Metadaten erhalten bleiben. Nicht verlustfrei überführbare Inhalte oder Funktionen sind nachvollziehbar auszuweisen.

Die Betriebsbereitschaft wird darüber hinaus anhand mindestens der nachstehenden funktionalen Abnahmekriterien geprüft. Die Prüfung erfolgt mit vom Auftraggeber bereitgestellten oder eigens erzeugten Testinhalten. Ein Kriterium ist erfüllt, wenn das beschriebene Ergebnis reproduzierbar erreicht wird.

Nr.	Prüffall	Erwartetes Ergebnis
F-01	Zentrale Vorgaben und Mandantentrennung nach Abschnitt 4.1	Eine im übergeordneten Mandanten angelegte verbindliche Vorgabe ist im nachgeordneten Mandanten nicht veränderbar; eine als Vorlage bereitgestellte Vorgabe kann organisationsbezogen angepasst werden. Eine spätere Änderung der zentralen Vorgabe wird weitergegeben; der Zeitpunkt der Übernahme ist erkennbar. Ein Nutzer eines nachgeordneten Mandanten erhält keinen Zugriff auf Inhalte eines anderen.

Nr.	Prüffall	Erwartetes Ergebnis
F-02	Aggregierte Auswertung nach Abschnitt 4.1	Der übergeordnete Mandant wertet den Umsetzungsstand mehrerer nachgeordneter Mandanten aggregiert aus, ohne Zugriff auf einzelne Feststellungen oder sonstige Einzelinhalte zu erhalten.
F-03	Eigene Kataloge und Bausteine nach Abschnitt 4.2	Ein berechtigter Fachadministrator legt ohne Mitwirkung des Auftragnehmers einen eigenen Katalog mit mindestens einer Anforderung an, versioniert und gibt ihn frei und ordnet ihn einem Objekt zu; eine frühere Fassung bleibt nachvollziehbar. Eine Anforderung aus einem vorhandenen Katalog wird übernommen; Herkunft und Abweichung gegenüber der Ursprungsfassung bleiben erkennbar.
F-04	Zuordnung von Nachweisen nach Abschnitt 4.2	Derselbe Nachweis wird Anforderungen aus mindestens zwei unterschiedlichen Regelwerken zugeordnet; eine Änderung des Nachweises bleibt an beiden Zuordnungen nachvollziehbar. Ein weiteres Regelwerk wird aufgenommen, ohne dass bestehende Zuordnungen neu aufgebaut werden müssen.
F-05	Rollen, Prüferzugang und Anmeldung nach Abschnitt 4.2	Für die Rollen zentrale Verwaltung, Mandantenverwaltung, Bearbeitung und Lesen wird je ein Zugang eingerichtet; die Rechte entsprechen der jeweiligen Rolle. Ein zeitlich befristeter lesender Prüferzugang erhält keine Änderungsrechte. Ein Zugang mit erweiterten Rechten wird nur mit Mehrfaktor-Authentifizierung zugelassen.
F-06	Risiko, Maßnahme und Nachweis nach Abschnitt 4.2	Ein Risiko wird bewertet, eine Maßnahme mit Verantwortlichkeit und Fälligkeit zugeordnet, deren Bearbeitungsstand geändert und ein Nachweis hinterlegt; die Änderungshistorie weist Zeitpunkt und handelnde Person aus. Nach Umsetzung der Maßnahme wird das Risiko erneut bewertet; ein verbleibendes Risiko wird mit Begründung, verantwortlicher Person und Geltungsdauer angenommen.
F-07	Strukturierte Erhebung nach Abschnitt 4.2	Eine strukturierte Erhebung wird an eine Person außerhalb der Lösung versandt, über einen geschützten Zugang beantwortet und die Antwort dem zuvor festgelegten Objekt zugeordnet.

Nr.	Prüffall	Erwartetes Ergebnis
F-08	Übernahme vorhandener Inhalte nach Abschnitt 4.2	Ein vom Auftraggeber bereitgestellter Testbestand wird in einem vom Auftragnehmer unterstützten Format übernommen. Die vereinbarten Inhalte, Zuordnungen und Metadaten stehen anschließend für Bearbeitung und Auswertung zur Verfügung; nicht übernommene Inhalte werden ausgewiesen. Bei automatisierter Übernahme sind Ausführungsstatus, Zeitpunkt, verarbeiteter Umfang und aufgetretene Fehler nachvollziehbar; ein fehlgeschlagener Lauf wird kontrolliert wiederholt.
F-09	Ausleitung nach Abschnitt 9.2	Ein zusammenhängender Datenbestand eines Testmandanten wird einschließlich seiner fachlichen Beziehungen und der für eine Weiterverarbeitung erforderlichen Metadaten ausgeleitet; er umfasst mindestens eine Kette aus Anforderung, Risiko, Maßnahme, Verantwortlichkeit, Nachweis und Bearbeitungsstand. Die Ausleitung erfolgt in einem offenen, dokumentierten oder allgemein verbreiteten Format und ist ohne Werkzeuge des Auftragnehmers auswertbar; nicht verlustfrei überführbare Inhalte werden ausgewiesen.
F-10	Notfallmanagement nach Abschnitt 4.2	Ein kritischer Prozess wird mit seinen Abhängigkeiten erfasst; die Auswirkungen eines Ausfalls werden analysiert und daraus Wiederanlauf- und Wiederherstellungsziele abgeleitet. Ein Notfallplan mit Verantwortlichkeiten wird zugeordnet und eine Übung einschließlich Ergebnis dokumentiert.
F-11	Dienstleisterverwaltung nach Abschnitt 4.2	Ein Dienstleister wird mit den wesentlichen Vertragsangaben erfasst und einem Prozess zugeordnet. Für ihn wird eine strukturierte Erhebung durchgeführt und zu einem späteren Zeitpunkt wiederholt; Antwort, Nachweis, festgestelltes Risiko und daraus abgeleitete Maßnahme bleiben dem Dienstleister zugeordnet.
F-12	Umgang mit KI-Funktionen nach Abschnitt 4.3	Enthält die Lösung Funktionen, die auf Verfahren der künstlichen Intelligenz beruhen: Die Funktion wird für einen Mandanten abgeschaltet; danach erfolgt dort keine Verarbeitung durch diese Funktion. Bei aktivierter Funktion ist ein erzeugter Vorschlag als solcher erkennbar und wird nicht ohne gesonderte Handlung einer berechtigten Person übernommen.

Nr.	Prüffall	Erwartetes Ergebnis
F-13	Regelwerke, Dokumentenlenkung und Audit nach Abschnitt 4.2	Ein mitgeliefertes Regelwerk wird einem Objekt zugeordnet und der Umsetzungsstand erfasst. Ein Dokument durchläuft die Lenkung von der Erstellung über die Freigabe bis zur Wiedervorlage. Ein Audit wird geplant, durchgeführt und mit Feststellungen abgeschlossen; die Ergebnisse stehen für die Managementbewertung zur Verfügung.
F-14	Archivierung und Auswertung nach Abschnitt 4.2	Ein abgeschlossener Eintrag wird archiviert und ist danach nicht mehr veränderbar. Über den Bestand werden eine Übersicht und ein Bericht erzeugt; Such-, Filter- und Sortierfunktionen liefern nachvollziehbare Ergebnisse.

4.6 Erprobung im Vergabeverfahren für Fachlos 3

Der Bieter stellt dem Auftraggeber im Vergabeverfahren eine betriebsbereite Umgebung zur Erprobung bereit, mit mindestens zehn Zugängen und mindestens drei Mandanten. Der Auftraggeber prüft darin die Anforderungen nach den Abschnitten 4.1 bis 4.4, insbesondere die Mandantenstruktur mit verbindlicher und anpassbarer Übernahme, die Anmeldung über die Identitätsverwaltung, die Abbildung eines Regelwerks einschließlich der Zuordnung von Nachweisen sowie die Auswertungen.

Die Umgebung wird den zur Erprobung zugelassenen Bietern zu gleichen Bedingungen abverlangt und für denselben Zeitraum bereitgestellt. Umfang, Zeitraum und Ablauf der Erprobung ergeben sich aus der Anlage 03.6, die Bewertungskriterien aus Ziffer 16.3 der Angebotsbedingungen und der Anlage 06; sie gelten für alle Bieter in gleicher Weise.

In die Umgebung werden keine Sozial- oder Gesundheitsdaten und keine sonstigen personenbezogenen Daten des Auftraggebers eingebracht. Der Auftraggeber verwendet ausschließlich eigens erzeugte Beispielinhalte. Der Bieter erhält keinen Zugriff auf Daten des Auftraggebers.

Die Bereitstellung der Umgebung wird nicht gesondert vergütet. Nach Abschluss des Verfahrens werden die Umgebungen der nicht berücksichtigten Bieter einschließlich aller eingebrachten Inhalte gelöscht; die Löschung ist dem Auftraggeber nachzuweisen.

Das Ergebnis der Erprobung geht nach Maßgabe des Wertungsmerkmals W-10 in die Angebotswertung ein. Der Auftraggeber kann die Umgebung des Bieters, auf dessen Angebot der Zuschlag erteilt wird, in den Wirkbetrieb überführen. In diesem Fall werden die während der Erprobung erstellten Konfigurationen und Inhalte übernommen; die Umgebung wird auf den vertraglich geschuldeten Stand gebracht. Ein Anspruch des Bieters auf Überführung besteht nicht.

4.7 Bewertungsrelevante Merkmale

Die nachstehenden Merkmale sind keine Mindestanforderungen. Ihre Erfüllung wird bewertet; ihr Fehlen führt nicht zum Ausschluss. Der Bieter erklärt je Merkmal, ob und in welcher Ausprägung er es erfüllt.

Nr.	Merkmal	Beschreibung
W-01	Übersichtsseite	Die Übersichtsseite kann je Nutzer angepasst werden; Inhalte und Anordnung sind auswählbar.
W-02	Bedienhilfen	Für häufig genutzte Arbeitsschritte stehen Tastenkürzel oder vergleichbare Bedienhilfen zur Verfügung.
W-03	Erscheinungsbild	Das Erscheinungsbild kann je Mandant an das der jeweiligen Organisation angepasst werden.
W-04	Weitere Regelwerke	Über die in Abschnitt 4.1 genannten hinaus sind weitere Anforderungskataloge bereits abgebildet und ohne zusätzlichen Aufwand nutzbar. Der Bieter benennt sie.
W-05	Vorbelegte Inhalte	Für die abgebildeten Regelwerke sind Maßnahmen, Nachweisvorlagen und Musterdokumente vorbelegt, die als Ausgangspunkt für die eigene Ausgestaltung dienen können.
W-06	Barrierefreiheit	Die Lösung erfüllt die Anforderungen der Norm EN 301 549 über das gesetzlich geforderte Maß hinaus. Der Bieter legt einen Prüfbericht oder eine Erklärung zur Barrierefreiheit vor.
W-07	Angriffserkennung	Über die Grundanforderung Q-08 (Abschnitt 7.2 Absatz 3) hinausgehende Abdeckung der Angriffserkennung, Korrelation über Komponenten hinweg sowie Organisation der Reaktion auf erkannte Angriffsversuche.
W-08 (entfällt)	entfällt	Das Merkmal entfällt. Seine Punkte sind nach der Anlage 06 anteilig auf die Merkmale W-01 bis W-07 verteilt. Die Angaben zum Preismodell nach Abschnitt 4.1 sind im Preisblatt (Anlage 07.3) weiterhin zu machen; sie werden nicht gesondert bewertet.
W-09	Zeitpunkt der Herstellung noch fehlender Funktionen	Bewertet wird der vom Bieter nach Abschnitt 4.5 verbindlich benannte Zeitpunkt, zu dem sämtliche bei Angebotsabgabe noch nicht vorhandenen, nach Kapitel 4 geschuldeten Funktionen bereitgestellt sind. Maßgeblich ist die Zeitspanne zwischen Zuschlag und vollständiger Bereitstellung dieser Funktionen. Ein früherer verbindlicher Bereitstellungszeitpunkt wird besser bewertet als ein späterer. Die Höchstfrist nach Abschnitt 4.5 bleibt unberührt. Sind sämtliche nach Kapitel 4 geschuldeten Funktionen bereits bei Angebotsabgabe vorhanden, wird dies für die Bewertung dem frühestmöglichen

Nr.	Merkmal	Beschreibung
		Bereitstellungszeitpunkt gleichgestellt. Gewertet wird ausschließlich der im Angebot verbindlich zugesagte und nach Abschnitt 4.5 zum Vertragsbestandteil werdende Zeitpunkt; Umsetzungskonzepte, Zwischenstände oder unverbindliche Beschleunigungsmöglichkeiten bleiben für dieses Merkmal außer Betracht. Die Bewertungsmethode und die Gewichtung werden in den Vergabeunterlagen festgelegt.
W-10	Ergebnis der Erprobung	Ergebnis der Erprobung nach Abschnitt 4.6. Bewertet werden die dort erhobenen Feststellungen zur Abbildung der Anforderungskataloge, zur Nachweis- und Maßnahmenverwaltung, zur Mandantentrennung und zur Bedienbarkeit. Maßgeblich sind die in der Erprobung erhobenen Werte und nicht die Darstellung im Angebot; der Bewertungsmaßstab wird mit den Vergabeunterlagen bekannt gegeben. Bietet ein Bieter eine nach Kapitel 4 geschuldete Funktion bei Angebotsabgabe noch nicht an, wird sie in der Erprobung als nicht vorhanden bewertet; der Zeitpunkt ihrer Herstellung bleibt Gegenstand des Merkmals W-09. Abweichend von der Einleitung dieses Abschnitts ist die Mandantentrennung Mindestanforderung: Wird sie in der Erprobung (Prüfschritt 3 der Anlage 03.6) nicht nachgewiesen, wird das Angebot ausgeschlossen.

4.8 Qualifikation des eingesetzten Personals

(1) Soweit Leistungen dieses Fachloses nach Tagessätzen abgerufen und abgerechnet werden, insbesondere die produktbezogenen Beratungs- und Unterstützungsleistungen und die Entwicklungsleistungen zur Anpassung der Standardkonfigurationen nach Abschnitt 4.1, werden sie durch Personen erbracht, die die nachstehenden Mindestanforderungen erfüllen. Der Auftragnehmer benennt je Profil die vorgesehenen Personen mit Qualifikation, Zertifizierungen und Referenzprojekten.

(2) Projektleitung: mindestens acht Jahre Berufserfahrung in der Leitung von Einführungs- oder Rolloutprojekten für Standardlösungen, davon einschlägige Erfahrung mit mandantenfähigen Lösungen.

(3) Beratung: mindestens drei Jahre Berufserfahrung in der produktbezogenen Beratung zu Einrichtung, Konfiguration und Nutzung von Lösungen zur Führung von Managementsystemen.

(4) Entwicklung: mindestens drei Jahre Berufserfahrung in der Anpassung und Erweiterung der Standardkonfigurationen solcher Lösungen innerhalb ihrer Konfigurations- und Erweiterungsmöglichkeiten.

(5) Erfahrung ist ein durch praktische Tätigkeit oder Befassung mit entsprechenden Projekten erworbener Wissensstand. 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. 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 der Leistungsbeschreibung jenes Fachloses auch weitere Anwendungen mit Komponenten der künstlichen Intelligenz und damit die Lösung dieses Fachloses, sobald deren Funktionen nach Abschnitt 4.3 aktiviert sind. Für die Fachlose 1 und 3 ist die Benennung derselben Person zulässig, soweit die zugesagte Verfügbarkeit gewahrt bleibt.

(6) Der Bieter weist im Preisblatt je Profil einen Tagessatz aus. Die für die Wertung maßgebliche Menge je Profil gibt das Preisblatt für alle Angebote gleich vor; eigene Mengenannahmen der Bieter werden nicht gewertet. Für die Zuordnung eines angebotenen Satzes zu einem Profil ist nicht die Bezeichnung beim Bieter maßgeblich, sondern die nachgewiesene Erfahrung und die vorgesehene Tätigkeit. Ein Profil, das eine höhere Erfahrungs- oder Verantwortungsstufe als die Projektleitung bezeichnet, begründet keinen weiteren Tagessatz. Leistungen, die dem Fachlos 2 zugeordnet sind, insbesondere die methodische Beratung zum Aufbau und Betrieb der Managementsysteme sowie Prüfleistungen, werden nicht über diese Profile abgerufen. Die im Angebot ausgewiesenen Tagessätze bleiben bis zum Wirksamwerden der ersten Anpassung zum 1. April 2029 unverändert. Die erste Anpassung erfasst ausschließlich die Indexentwicklung zwischen den Jahresdurchschnitten 2027 und 2028; Indexentwicklungen bis einschließlich 2027 sind einzukalkulieren. Für die restliche Vertragslaufzeit sieht der Vertrag eine Anpassungsregelung vor, die sich an einer veröffentlichten Indexreihe des Statistischen Bundesamtes orientiert, Anpassungen nach oben und nach unten in gleicher Weise zulässt, einmal je Kalenderjahr zum 1. April, frühestens zum 1. April 2029, wirkt und je Anpassungsschritt auf drei vom Hundert begrenzt ist; Einzelheiten, insbesondere die maßgebliche Indexreihe, der maßgebliche Erhebungszeitraum, ein Schwellenwert und das Verfahren bei Umstellung des Basisjahres oder Wegfall der Reihe, regelt der Vertrag.

4.9 Erweiterung des Leistungsumfangs

(1) Die Erweiterungen nach diesem Abschnitt gehören nicht zur Grundleistung und nicht zu dem nach Kapitel 4 geschuldeten Leistungsumfang. Die abrufende Stelle kann sie nach Maßgabe der nachstehenden Bestimmungen beauftragen; eine Pflicht hierzu besteht nicht. Ein Anspruch des Auftragnehmers auf Beauftragung einer Erweiterung besteht nicht. Eine Erweiterung ist nicht Voraussetzung der Betriebsbereitschaft nach Abschnitt 4.5 und erweitert den Mindestumfang des nach Kapitel 3 abgerufenen Mandanten nicht.

(2) Gegenstand einer Erweiterung können assistierende Funktionen sein, die über die Führung des Managementsystems hinaus bei der Umsetzung offener Anforderungen unterstützen. In Betracht kommen: die Ermittlung und Priorisierung noch offener Anforderungen, Maßnahmen und Nachweise anhand des im Mandanten geführten Stands; die selbsttätige Aufforderung der jeweils zuständigen Beschäftigten zur Mitwirkung über einen von der abrufenden Stelle bereits genutzten Kommunikations- oder Kollaborationsdienst und die Rückführung der Rückmeldungen in das Managementsystem; die strukturierte Erhebung an eine Person außerhalb der Lösung über einen geschützten Zugang gehört nach Abschnitt 4.2 und dem Prüffall F-07 des Abschnitts 4.5 zur Grundleistung und ist nicht Gegenstand einer Erweiterung; die Unterstützung bei der Modellierung nach einem der Anforderungskataloge des Abschnitts 4.1 einschließlich der Zuordnung von Anforderungen, Werten und Maßnahmen; sowie die Einbindung dieser Unterstützung in die Verwaltung der Werte und in die Bearbeitung von Vorfällen. Die Beschreibung ist funktional zu verstehen; maßgeblich ist das beschriebene Ergebnis und nicht ein bestimmtes Erzeugnis, Verfahren oder Betriebsmodell. Gegenstand einer Erweiterung ist allein der

über die Grundleistung hinausgehende Anteil: dass die Funktion den offenen Stand selbst ermittelt und den Anlass für die Mitwirkung selbst bestimmt. Leistungen, die nach den Abschnitten 4.1 bis 4.5 geschuldet sind, werden nicht als Erweiterung vergütet.

(3) Für Erweiterungen nach Absatz 2 gilt Abschnitt 4.3 vollständig, auch soweit sie nicht auf Verfahren der künstlichen Intelligenz beruhen. Sie werden je Mandant durch die Administration dieses Mandanten abgeschaltet und sind im Auslieferungszustand deaktiviert. Die Zuständigkeit für fachliche Feststellungen, Bewertungen und Freigaben bleibt bei den Beschäftigten der abrufenden Stelle.

(4) Für Erweiterungen gilt kein gesonderter Höchstwert; ihr Wert ist im Höchstwert der Rahmenvereinbarung enthalten. Die abrufende Stelle zeigt jede beabsichtigte Beauftragung dem Auftraggeber vor der Beauftragung an. Der Auftraggeber führt den verbrauchten und den verbleibenden Wert der Rahmenvereinbarung; eine Beauftragung ist nur zulässig, soweit der verbleibende Wert ausreicht. Das Verfahren regelt die Rahmenvereinbarung.

(5) Die Erweiterungen beziehen sich auf die im jeweiligen Einzelvertrag eingesetzte Lösung. Die Beauftragung erfolgt gegenüber dem Auftragnehmer dieses Einzelvertrags zu den im Vergabeverfahren festgelegten Preisen. Ein Mini-Wettbewerb findet nach Kapitel 3 für dieses Fachlos nicht statt. Es entscheidet die Stelle, die den Einzelvertrag geschlossen hat; sie kann die Erweiterungen einzeln, gemeinsam oder nacheinander beauftragen und ist hierzu nicht verpflichtet. Die vergabe- und vertragsrechtliche Umsetzung verantwortet die abrufende Stelle; dazu gehört die Beachtung der für sie geltenden Wertgrenzen. Nach Ende des Einzelvertrags gelten für einen neuen Abruf die Regelungen des Kapitels 3 erneut.

(6) Der Bieter weist im Preisblatt für die Erweiterungen nach Absatz 2 einen Preis je Mandant und Jahr aus. Der Preis umfasst Einrichtung, Betrieb und Pflege sowie die Anbindung an den Dienst nach Absatz 2; eine gesonderte Einrichtungsvergütung wird nicht vorgesehen. Die Erweiterungen nach Absatz 2 sind zwingend anzubieten; einzutragen ist ein Preis größer als 0,00 Euro, eine Kennzeichnung als nicht angeboten ist nicht zulässig. Der Preis geht mit der im Preisblatt vorgegebenen Wertungsmenge von zehn Mandantenjahren (fünf Mandanten über zwei Jahre) in die Wertungssumme ein; die Wertungsmenge begründet keine Abnahmepflicht und keinen Abrufanspruch.

(7) Der Bieter beschreibt mit dem Angebot, welche Funktionen er für die Erweiterungen nach Absatz 2 einsetzt, welche Daten dabei verarbeitet werden, an welche Dienste außerhalb der Lösung Angaben übermittelt werden, welche Empfängerkreise und Datenarten davon erfasst sind und an welchen Standorten die Verarbeitung erfolgt. Für die Verarbeitung personenbezogener Daten gelten die Kapitel 6 bis 9 und der Vertrag über die Auftragsverarbeitung. Das in der Rahmenvereinbarung geregelte Änderungsverfahren bleibt unberührt.

Teil III – Gemeinsame Bestimmungen

5 Geltungsbereich der gemeinsamen Bestimmungen

Die Kapitel dieses Teils gelten für den Auftragnehmer dieses Fachloses. Sie beschreiben die Anforderungen an den von ihm betriebenen Dienst und sind unabhängig davon zu erfüllen, welche fachliche Leistung er erbringt.

Soweit die nachfolgenden Anforderungen auf Fälle, Fallkontexte, Zusammenfassungen, Dialogfunktionen oder Komponenten der künstlichen Intelligenz Bezug nehmen, gelten sie sinngemäß für die in der Lösung verarbeiteten Daten, Bearbeitungsschritte und Funktionen; enthält die Lösung keine Funktionen, die auf Verfahren der künstlichen Intelligenz beruhen, entfallen die darauf bezogenen Anforderungen.

Losspezifische Regelungen im Kapitel 4 gehen vor, soweit sie weitergehende Anforderungen enthalten.

5.1 Geltungsbereich und Schutzbedarf

(1) Die Anforderungen der Kapitel 5 bis 10 gelten für sämtliche Komponenten der Lösung, unabhängig davon, ob sie beim Auftragnehmer oder bei Dritten betrieben werden.

(2) Sie gelten gleichermaßen für alle Unterauftragnehmer, Modellanbieter, Infrastruktur- und Supportdienstleister, 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. Der Auftragnehmer unterstützt dessen Aufbau und Betrieb, indem er die hierfür erforderlichen Angaben und Unterlagen bereitstellt, insbesondere zur Zweckbestimmung, zur Risikobewertung, zu bekannten Einschränkungen und Fehlerarten, zur Datenverarbeitung sowie zur Protokollierung. 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.

(6) Die Leistung wird als vom Auftragnehmer betriebener Dienst im Sinne von Software als Dienstleistung (Software as a Service) erbracht. Die Bezeichnung betrifft den Leistungsinhalt, nämlich die betriebsbereite Bereitstellung einschließlich Betrieb, Pflege und Verfügbarkeit, und nicht den Ort des Betriebs. Betrieb, Wartung und Absicherung der zur Leistungserbringung eingesetzten Komponenten

obliegen dem Auftragnehmer, einschließlich der von ihm beauftragten Infrastruktur- und Plattformdienstleister. Die Betriebsumgebung stellt der Auftragnehmer bereit und kalkuliert sie; das umfasst Rechen- und Speicherressourcen, Betriebssysteme, Laufzeitumgebungen und die erforderlichen Lizenzen. Die Komponenten werden beim Auftragnehmer oder bei einem oder mehreren von ihm beauftragten Dienstleistern betrieben. Eine Installation von Komponenten in den Räumlichkeiten oder der Infrastruktur des Auftraggebers, eines Bedarfsträgers oder eines von diesen beauftragten Dienstleisters ist nicht Gegenstand der Leistung. Der Auftragnehmer benennt mit dem Angebot für jede Komponente den Betriebsort und jeden beteiligten Dritten und grenzt die Verantwortlichkeiten ab. Die Verarbeitung findet ausschließlich innerhalb des Europäischen Wirtschaftsraums statt; bei beteiligten Dritten erfolgt keine dauerhafte Speicherung. Die Trennung der Mandanten wird über die gesamte Verarbeitungskette einschließlich ausgelagerter Verarbeitungsschritte durchgehalten und auf Verlangen nachgewiesen.

(7) 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, zeigt dem Auftraggeber daraus folgenden Anpassungsbedarf unaufgefordert an und setzt ihn in einem dokumentierten Änderungs- und Freigabeverfahren um. Die Anpassung an den fortgeschriebenen Stand der Technik ist Teil der geschuldeten Leistung, soweit sie den bestehenden Leistungsumfang erhält; das gilt insbesondere für Aktualisierungen von Verfahren, Verschlüsselung, Härtung und Abhängigkeiten. Erfordert eine geänderte Vorgabe eine neue Funktion, eine Änderung der Architektur oder einen sonstigen wesentlichen Zusatzaufwand, so wird sie über das im Rahmenvertrag geregelte Änderungsverfahren vereinbart.

(8) Für dieses Fachlos wird die Rahmenvereinbarung mit einem Unternehmen geschlossen; der Fall mehrerer Rahmenvertragspartner tritt nicht ein. Nachweise, Konzepte und Erklärungen sind einmalig auf Ebene der Rahmenvereinbarung zu erbringen und je Abruf um die abrufspezifischen Angaben zu ergänzen; eine erneute vollständige Vorlage je Abruf ist nicht erforderlich.

6 Architektur, Zugriffsschutz und Trennung der Daten

6.1 Identitäts- und Berechtigungsmanagement

(1) Die Lösung darf Inhalte eines Mandanten nur verarbeiten oder anzeigen, wenn der angemeldete Nutzer für diesen Mandanten und für den betroffenen Gegenstand des Managementsystems berechtigt ist. Die Berechtigungsprüfung erfolgt serverseitig und unabhängig von den im Aufruf übergebenen Parametern. Sie umfasst sämtliche im Rollenkonzept nach Abschnitt 4.2 geführten Berechtigungsmerkmale. Eine Prüfung ausschließlich in der Oberfläche genügt nicht.

(2) Die Anmeldung erfolgt nach Abschnitt 4.2; der übergebene Anmeldekontext ist integritätsgeschützt und authentisiert und enthält mindestens Nutzeridentität, Mandant, Rollen und einen Gültigkeitszeitraum. Wiedereinspielung und Manipulation des Aufrufs werden wirksam verhindert.

(3) Eine Veränderung von Aufrufparametern, Kennungen, URL-Bestandteilen oder API-Aufrufen eröffnet keinen Zugriff auf Inhalte eines anderen Mandanten und keine weitergehenden Rechte innerhalb des eigenen Mandanten.

(4) Entzogene, abgelaufene oder geänderte Berechtigungen wirken sich unverzüglich auf laufende und neue Sitzungen aus. Ein Entzug wird spätestens innerhalb von fünf Minuten wirksam; laufende Sitzungen werden beendet. Der Auftragnehmer weist die tatsächliche Wirkdauer nach.

(5) Die Lösung beendet Sitzungen nach fünfzehn Minuten Inaktivität sowie nach einer absoluten Höchstdauer von zehn Stunden und verlangt danach eine erneute Authentifizierung. Sitzungskennungen werden bei der Anmeldung neu vergeben, sind nicht vorhersagbar und werden bei Abmeldung serverseitig ungültig. Eine Abmeldemöglichkeit ist in der Oberfläche jederzeit erreichbar.

(6) Der Zugriff auf Auswertungen, Berichte und archivierte Inhalte unterliegt derselben Berechtigungsprüfung wie der Zugriff auf die zugrunde liegenden Gegenstände des Managementsystems.

(7) Für administrative, betriebliche und unterstützende Zugriffe bestehen von den Fachrollen getrennte Berechtigungen nach dem Grundsatz der geringsten Rechte. Privilegierte Zugriffe erfolgen ausschließlich unter Verwendung von Mehrfaktor- oder kontinuierlicher Authentifizierung.

(8) Berechtigungen und Rollen werden durch berechtigte Beschäftigte des Auftraggebers oder des jeweiligen Bedarfsträgers für ihren jeweiligen Verantwortungsbereich selbst vergeben, geändert und entzogen. Eine Mitwirkung des Auftragnehmers ist hierfür nicht erforderlich. Die Lösung unterstützt die Hinterlegung von Stellvertretungen sowie die Vergabe von Berechtigungen mit Gültigkeitsdauer; nach Ablauf enden sie ohne weiteres Zutun.

(9) Der Auftraggeber und jeder Bedarfsträger können die in ihrem Bereich vergebenen Berechtigungen jederzeit auswerten und in einem wiederkehrenden Verfahren überprüfen. Die Lösung stellt hierfür eine Übersicht bereit, aus der je Nutzer die zugewiesenen Rollen, deren Geltungsdauer und der Zeitpunkt der letzten Änderung hervorgehen. Nicht mehr benötigte Berechtigungen können in diesem Verfahren entzogen werden. Vergabe, Änderung und Entzug von Berechtigungen werden mit Zeitpunkt, handelnder Person und betroffener Nutzerkennung protokolliert.

(10) Zugänge für Not- und Ausnahmefälle, die erweiterte Rechte gewähren, sind auf das Notwendige beschränkt, zeitlich befristet und an eine gesonderte Freigabe gebunden. Ihre Einrichtung, Nutzung und Beendigung wird personenbezogen protokolliert und dem betroffenen Bedarfsträger sowie dem Auftraggeber unverzüglich angezeigt.

(11) Jede systemseitig ausgelöste Aktion mit lesender oder schreibender Wirkung auf Inhalte eines Mandanten ist einer eindeutigen technischen Identität zugeordnet. Sammelidentitäten und geteilte Systemkonten sind für solche Aktionen unzulässig. Die Zuordnung wird nach Abschnitt 7.1 protokolliert und ist für die Stelle auswertbar, die den betroffenen Mandanten führt.

(12) Die Berechtigungsregeln werden serverseitig für jede Operation und jedes betroffene Datenobjekt durchgesetzt. Eine pauschale Berechtigung auf Sitzungs- oder Systemkontoebene genügt nicht; eine erneute Anmeldung des Nutzers je Aktion ist nicht gefordert. Der Auftragnehmer stellt dem jeweiligen Bedarfsträger mindestens jährlich eine Auswertung der vergebenen Berechtigungen bereit, die dessen Überprüfung der fachlichen Erforderlichkeit ermöglicht; die Bestätigung erteilt der Bedarfsträger.

(13) Für technische Komponenten werden kurzlebige, an den jeweiligen Verarbeitungsvorgang gebundene Zugangsmittel verwendet, soweit die eingesetzten Verfahren dies zulassen. Dauerhaft

hinterlegte Zugangsdaten und Berechtigungen, die über den konkreten Verwendungszweck hinausgehen, werden vermieden; ihre Verwendung ist zu begründen und von der Stelle freizugeben, in deren Verantwortungsbereich sie eingesetzt werden.

6.2 Verschlüsselung und Schlüsselmanagement

(1) Personenbezogene Daten, Sozialdaten und Gesundheitsdaten sind bei der Übertragung und bei der Speicherung zu verschlüsseln. Dies gilt auch für Sicherungen, Protokolle, Zwischenspeicher, Such- und Vektorindizes. Für Verfahren, Betriebsarten und Schlüssellängen der Speicherverschlüsselung ist die Technische Richtlinie BSI TR-02102-1 in der jeweils geltenden Fassung maßgeblich; einzusetzen sind Verfahren mit authentifizierter Verschlüsselung.

(2) Für die Transportverschlüsselung ist TLS in der Version 1.3 einzusetzen. TLS 1.2 ist nur übergangsweise und nur mit Verfahren zur authentifizierten Verschlüsselung sowie mit Perfect Forward Secrecy zulässig; der Auftragnehmer weist die Notwendigkeit nach und benennt einen Termin für die Ablösung. Ältere Protokollversionen sowie Betriebsarten ohne authentifizierte Verschlüsselung sind deaktiviert. Maßgeblich für Protokollversionen, Verfahren und Schlüssellängen ist die Technische Richtlinie BSI TR-02102-2 in der jeweils geltenden Fassung. Webbasierte Oberflächen sind gegen die Umgehung der Transportverschlüsselung abzusichern. Bei einer Fortschreibung der Technischen Richtlinie passt der Auftragnehmer die Konfiguration in einem dokumentierten Änderungs- und Freigabeverfahren an.

(3) Eine Verschlüsselung der Inhalte der Mandanten auf Anwendungsebene, die über die Verschlüsselung nach den Absätzen 1 und 2 hinausgeht, wird nicht verlangt. Der Auftragnehmer benennt stattdessen alle Stellen der Verarbeitungskette, an denen Inhalte der Mandanten im Klartext vorliegen, und grenzt die für die fachliche Verarbeitung bestimmte Vertrauenszone ab. Komponenten außerhalb dieser Zone, insbesondere Infrastruktur- und Plattformdienstleister des Auftragnehmers, dürfen Inhalte der Mandanten nicht im Klartext verarbeiten; an Zwischenstationen, an denen die Transportverschlüsselung terminiert wird, ist allein die Weiterleitung ohne fachliche Verarbeitung zulässig. Der Auftragnehmer stellt die Grenze der Vertrauenszone, die Stellen der Entschlüsselung und die innerhalb der Zone zugriffsberechtigten Komponenten im Verschlüsselungs- und Schlüsselkonzept dar. Die Verschlüsselung nach den Absätzen 1 und 2 schuldet der Auftragnehmer in jedem Fall. Verlangt eine abrufende Stelle darüber hinaus, die Hoheit über die Schlüssel der Speicherverschlüsselung oder über die für die Transportverschlüsselung eingesetzten Zertifikate selbst auszuüben, so unterstützt der Auftragnehmer dies; die technische Ausgestaltung vereinbaren die Parteien im Einzelvertrag, insbesondere Bereitstellung, Aufbewahrung, Wechsel und Widerruf der Schlüssel, die Entsperrung nach einem Neustart, einer Wartung oder einer Wiederherstellung und die dafür erforderliche Mitwirkung der abrufenden Stelle. Der Auftragnehmer legt mit dem Angebot dar, in welcher Form er diese Ausgestaltung anbieten kann, welche Mitwirkung er dafür benötigt und welche Folgen ein Widerruf oder Verlust eines Schlüssels für die Lesbarkeit der betroffenen Bestände und für den Wiederanlauf hat. Soweit die Entsperrung von einer Mitwirkung der abrufenden Stelle abhängt, gehen hierauf beruhende Verzögerungen nicht zu Lasten des Auftragnehmers.

(4) Die Lösung ist kryptoagil auszulegen: Verwendete Verfahren, Schlüssellängen und Protokollversionen sind konfigurierbar und ohne Eingriff in den Programmcode austauschbar. Der Auftragnehmer legt dar, wie ein Wechsel kryptographischer Verfahren durchgeführt wird und welche Vorlaufzeit er benötigt. Er beobachtet die Entwicklung zu quantensicheren Verfahren und zeigt dem Auftraggeber

rechtzeitig an, wann und in welchem Umfang eine Umstellung auf hybride oder quantensichere Schlüsseleinigungsverfahren erforderlich wird.

(5) Der Auftragnehmer beschreibt eingesetzte Protokolle und Verfahren, Schlüsselerzeugung, Schlüsselaufbewahrung, Schlüsselwechsel, Sperrung kompromittierter Schlüssel, Zertifikatsverwaltung sowie die Trennung zwischen Mandanten und zwischen Produktiv-, Test- und Schulungsumgebungen.

(6) Der Auftragnehmer benennt eindeutig, welche Stelle die Schlüssel kontrolliert: der Auftraggeber, die abrufende Stelle, eine von ihnen bestimmte Stelle, der Auftragnehmer oder ein Infrastrukturdienstleister. Für jede Schlüsselart sind Inhaberschaft, Zugriffsberechtigte und Verfahren im Fall der Vertragsbeendigung anzugeben.

(7) Eine Entschlüsselung durch den Auftragnehmer, seine Unterauftragnehmer oder Infrastrukturdienstleister außerhalb der zur Leistungserbringung erforderlichen Verarbeitungsschritte ist ausgeschlossen und technisch zu verhindern oder nachweisbar zu machen.

6.3 Datenhaltung, Speicherfristen und Löschung

(1) Der Auftragnehmer legt je Komponente und je Datenart offen, ob eine dauerhafte, temporäre oder ausschließlich flüchtige Verarbeitung erfolgt. Zu erfassen sind mindestens die Inhalte der Managementsysteme einschließlich Dokumenten, Nachweisen, Risiko- und Maßnahmenregistern, Auditunterlagen und Erhebungen, hochgeladene Dateien und daraus extrahierte Texte, Such- und Indexdaten, Auswertungs- und Berichtsdaten, Protokolle sowie Telemetrie- und Fehlerdiagnosedaten. Setzt die Lösung Funktionen nach Abschnitt 4.3 ein, sind zusätzlich Prompts und Kontextdaten, Einbettungen und Vektordaten sowie die von diesen Funktionen erzeugten Vorschläge zu erfassen.

(2) Je Datenart sind anzugeben: Speicherort, Speicherzweck, Speicherdauer, Löschverfahren, Zugriffsberechtigte, Verschlüsselung, Behandlung in Sicherungen und Übermittlung an Unterauftragnehmer.

(3) Der Auftragnehmer erklärt, ob die Lösung Such- oder Vektorindizes betreibt, die über mehrere Mandanten hinweg gemeinsam genutzt werden. Er benennt, wo diese betrieben werden, welche Inhalte sie enthalten und wie die Mandantentrennung nach Abschnitt 4.1 durchgesetzt wird. Eine gemeinsam genutzte Infrastruktur ist zulässig, soweit die Inhalte je Mandant getrennt bleiben; eine mandantenübergreifende Auswertung ist nur in der aggregierten Form des Abschnitts 4.1 zulässig. Entsteht darüber hinaus ein mandantenübergreifend auswertbarer Bestand, ist er als eigenständige Verarbeitung zu behandeln und gesondert zu begründen.

(4) Die Löschung muss manuell, teilautomatisiert und vollautomatisiert möglich sein. Zusätzlich muss eine Sperrung von Datensätzen möglich sein, die den weiteren Zugriff unterbindet, ohne die Daten zu löschen. Löschregeln und Fristen müssen an geänderte rechtliche Vorgaben angepasst werden können, ohne dass ein Eingriff in den Programmcode erforderlich ist.

(5) Die Lösung ermöglicht die revisionssichere Archivierung nach Abschnitt 4.2 und die Löschung archivierter Inhalte auf Weisung der für die Verarbeitung verantwortlichen Stelle unter Protokollierung des Vorgangs.

(6) Die Speicherdauer der Inhalte eines Mandanten bestimmt die Stelle, die diesen Mandanten führt. Für die Rückgabe und Löschung bei Vertragsende sowie bei Beendigung der Nutzung durch einen einzelnen Mandanten gilt Abschnitt 9.2.

(7) Der Auftragnehmer beschreibt das Verfahren einschließlich der Behandlung fehlgeschlagener Übermittlungen und weist die Löschung nach.

6.4 Netzsicherheit und Segmentierung

(1) Der Auftragnehmer legt ein Zonenmodell mit Vertrauenszonen, Zonenübergängen und Filterregeln vor. Fach-, Verwaltungs-, KI- und Datenhaltungskomponenten sind unterschiedlichen Zonen zuzuordnen.

(2) Administrative Zugriffe erfolgen über von den Fachzugriffen getrennte Netzwege oder über eine technisch gleichwertige, vom Auftragnehmer nachzuweisende Trennung. Eine Administration über dieselben Wege wie der fachliche Zugriff ohne zusätzliche Trennungsmaßnahme ist unzulässig.

(3) Externe Verbindungen erfolgen ausschließlich verschlüsselt und authentisiert, sind auf die notwendigen Gegenstellen begrenzt und vollständig dokumentiert.

(4) Auch Verbindungen zwischen den Komponenten der Lösung, einschließlich der Verbindungen zu Datenhaltung, Such- und Vektorindizes, Protokollierung und Komponenten der künstlichen Intelligenz, erfolgen verschlüsselt und beidseitig authentisiert. Eine unverschlüsselte Übertragung innerhalb der Betriebsumgebung ist nur zulässig, soweit sie technisch unvermeidbar ist; der Auftragnehmer benennt und begründet solche Fälle.

(5) KI- und Retrieval-Komponenten sind in einer eigenen Zone oder in einer technisch gleichwertigen, vom Auftragnehmer nachzuweisenden Isolation zu betreiben. Ausgehende Kommunikation ist auf eine dokumentierte Positivliste freigegebener Ziele beschränkt; alle übrigen Verbindungen werden unterbunden und protokolliert.

(6) Änderungen an Zonenmodell, Filterregeln und Positivlisten unterliegen einem dokumentierten Änderungsverfahren.

(7) Komponenten zur Verarbeitung nicht vertrauenswürdiger Inhalte sowie die KI- und Retrieval-Komponenten haben keinen Zugriff auf Metadatendienste der Betriebsplattform, auf Verwaltungsschnittstellen der Host- oder Knotenebene, auf Steuerungsebenen von Orchestrierungssystemen und auf vergleichbare Infrastrukturendpunkte. Erforderliche Ausnahmen werden je Komponente begründet, auf die notwendigen Operationen beschränkt und vom Auftraggeber freigegeben.

(8) Die Freigabe ausgehender Verbindungen erfolgt nicht allein nach Zieladresse, sondern ist an Zweck, Protokoll, Dienst, Ressource und zulässige Operationen gebunden; lässt ein eingesetztes Verfahren diese Bindung nicht zu, beschreibt der Auftragnehmer die stattdessen wirksamen Maßnahmen. Die Freigabe eines Zielsystems berechtigt insbesondere nicht zur Nutzung seiner Upload-, Schreib-, Ablage- oder Nachrichtenfunktionen.

6.5 Konfigurations- und Härtungsmanagement

(1) Der Auftragnehmer dokumentiert je Komponententyp eine Sicherheitsbaseline auf Grundlage anerkannter Härtungsvorgaben in der jeweils geltenden Fassung und setzt sie um. Abweichungen sind zulässig, soweit sie dokumentiert, risikobewertet und vom Auftraggeber genehmigt sind. Bei Fortschreibung der zugrunde liegenden Vorgaben aktualisiert der Auftragnehmer die Baseline und zeigt dies dem Auftraggeber an.

(2) Systeme und Anwendungen werden nach einem anerkannten, veröffentlichten Härtungsmaßstab konfiguriert; in Betracht kommen insbesondere die einschlägigen Bausteine des IT-Grundschutz-Kompendiums des Bundesamts für Sicherheit in der Informationstechnik oder gleichwertige Vorgaben. Der Auftragnehmer benennt den verwendeten Maßstab. Nicht benötigte Dienste, Schnittstellen, Protokolle, Beispieldaten und Standardkonten werden deaktiviert oder entfernt.

(3) Voreingestellte Zugangsdaten werden vor Inbetriebnahme geändert. Der Auftragnehmer weist dies nach.

(4) Abweichungen von der Baseline werden automatisiert erkannt, protokolliert und dem Auftraggeber in auswertbarer Form gemeldet.

(5) Konfigurationsstände sind versioniert und Änderungen nachvollziehbar; sie unterliegen einem dokumentierten Änderungsverfahren.

6.6 Fernwartung und administrative Zugänge

(1) Fernzugriffe erfolgen ausschließlich über vom Auftraggeber freigegebene Verfahren, verschlüsselt, mehrfaktorauthentisiert und zeitlich begrenzt.

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

(3) Endgeräte für Fernwartung unterliegen definierten Anforderungen an Verschlüsselung, Patchstand und Schadsoftwareschutz und werden nicht für private Zwecke genutzt.

(4) Fernwartungssitzungen werden vollständig protokolliert. Der Auftraggeber und der betroffene Bedarfsträger können Sitzungen mitverfolgen.

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

6.7 Physische Sicherheit extern betriebener Komponenten

(1) Der Auftragnehmer benennt sämtliche Standorte, an denen Komponenten mit Bezug zu Daten des Auftraggebers und der Bedarfsträger betrieben werden, und weist die physische Sicherheit nach: Zutrittskontrolle, Überwachung, Brandschutz, Stromversorgung, Klimatisierung. Werden Rechenzentren

Dritter genutzt, genügt für diesen Nachweis deren Zertifizierung oder ein gleichwertiges Testat, soweit Geltungsbereich und Prüfzeitraum den konkret genutzten Standort erfassen; der Auftragnehmer legt die entsprechenden Unterlagen vor. Standortangaben und Nachweise sind mit dem Angebot vorzulegen; sie sind bei Ablauf, bei Wechsel eines Standorts und bei Änderung des Geltungsbereichs unaufgefordert zu aktualisieren.

(2) Datenträger mit Daten des Auftraggebers und der Bedarfsträger werden verschlüsselt, bestandsgeführt und nach einem anerkannten Verfahren vernichtet. Die Vernichtung wird nachgewiesen.

(3) Transport oder Versand von Datenträgern mit Daten des Auftraggebers und der Bedarfsträger erfolgt nur mit vorheriger Zustimmung der Stelle, in deren Verantwortungsbereich die Daten liegen, und zusätzlich des Auftraggebers.

7 Protokollierung und Überwachung

7.1 Protokollierung und Beweissicherung

(1) Protokolliert werden mindestens: An- und Abmeldung, Aufruf von Gegenständen des Managementsystems und von Registern, Dokumentzugriff, Erstellung, Änderung, Freigabe und Außerkraftsetzung von Inhalten, Datenexporte, Abrufe von Auswertungen und Berichten einschließlich Filter- und Zeitraumangaben, fehlgeschlagene Zugriffs- und Anmeldeversuche, Berechtigungs- und Rollenänderungen, Änderungen an der Konfiguration eines Mandanten und an den verbindlich zu übernehmenden Vorgaben des übergeordneten Mandanten, administrative und unterstützende Zugriffe, Sperrung und Löschung von Datensätzen einschließlich der Löschungen nach Abschnitt 6.3 sowie sicherheitsrelevante Ereignisse. Setzt die Lösung Funktionen nach Abschnitt 4.3 ein, werden zusätzlich deren Aufrufe und die Änderungen an Modellen, Prompts und Konfigurationen protokolliert.

(2) Je Ereignis werden mindestens erfasst: Zeitpunkt, Nutzeridentität, Mandant, betroffener Gegenstand des Managementsystems, ausgelöste Funktion, einbezogene Dokumente sowie Version der Lösung; bei Funktionen nach Abschnitt 4.3 zusätzlich die Version des Modells und der Prompt-Konfiguration. Bei einer Sperrung oder Löschung von Datensätzen werden zusätzlich die veranlassende Stelle und die Grundlage der Veranlassung erfasst, also die Weisung, die Löschregel oder die Fristbestimmung, auf der sie beruht. Löst keine Person das Ereignis aus, tritt die veranlassende Stelle an die Stelle der Nutzeridentität nach Satz 1. Die Aufzeichnung muss die Rekonstruktion des Zustandekommens einer Ausgabe ermöglichen. Die Protokolleinträge bleiben für die Dauer nach Absatz 6 auswertbar und dem betroffenen Gegenstand des Managementsystems zuordenbar, auch wenn dieser zwischenzeitlich gelöscht worden ist. Dadurch bleibt feststellbar, welche Person zu welchem Zeitpunkt welchen Stand eingesehen hat.

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

(4) Protokolle sind gegen Veränderung und Löschung durch Personal des Auftragnehmers und seiner Unterauftragnehmer geschützt und werden auf eine gemeinsame, verlässliche Zeitquelle synchronisiert. Zugriffe auf Protokolle werden ihrerseits protokolliert. Setzt die Lösung Funktionen nach Abschnitt 4.3 ein, so gilt ergänzend: Werkzeug-, Schnittstellen- und Fremdsystemaufrufe werden

einschließlich der zur Nachvollziehbarkeit erforderlichen Aufrufparameter, Ergebniskennungen, Statusangaben und der tatsächlich ausgelösten Systemwirkung durch die ausführende Instanz außerhalb der Ausführungsumgebung dieser Funktionen aufgezeichnet; die Funktionen haben auf diese Aufzeichnung weder schreibenden noch löschenden Zugriff. Enthalten Aufrufparameter oder Rückgabewerte Dokumentinhalte oder Gesundheitsdaten, so werden diese nach Absatz 3 nicht in die Protokolle übernommen; ihr Bezug wird über Kennungen und Fundstellenverweise hergestellt. Die Aufzeichnung muss die tatsächlich ausgeführte Aktion und ihre Auswirkung auch in diesem Fall unabhängig von Angaben dieser Funktionen nachvollziehbar machen. Deren Darstellungen über ihre eigene Aktivität gelten nicht als Nachweis.

(5) Jeder administrative Zugriff auf Systeme, Daten, Modelle oder Konfigurationen des Auftraggebers oder eines Bedarfsträgers, vor Ort oder aus der Ferne, ist personenbezogen zu protokollieren, einschließlich Zweck und Auftragsbezug.

(6) Die Protokolle werden bis zu zwölf Monate aufbewahrt. Die Dauer ist je Mandant und je Protokollart konfigurierbar; eine längere Aufbewahrung ist nur bei besonderem, dokumentiertem Bedarf und auf Weisung der verantwortlichen Stelle zulässig. Die Löschregeln gibt die Stelle vor, die den jeweiligen Mandanten führt, innerhalb dieser Obergrenze. Der Auftragnehmer benennt im Rahmen der Offenlegung nach Abschnitt 6.3 Absatz 1 und 2 die Protokollarten je Komponente der Lösung. Diese Angabe ist Bezugsgröße für die Konfiguration nach Satz 2 und für die Abnahme nach Abschnitt 4.5. Der Auftragnehmer beschreibt die technische Umsetzung sowie die Schnittstelle, über die die Stelle, die den jeweiligen Mandanten führt, die ihrem Verantwortungsbereich zugeordneten Protokolle auswerten oder in eigene Auswertungssysteme überführen kann.

(7) Eine Auswertung der Protokolle zur individuellen Verhaltens- oder Leistungskontrolle ist ausgeschlossen. Auswertungen zu Betriebs- und Qualitätszwecken erfolgen aggregiert und nach Vorgabe der für die Verarbeitung verantwortlichen Stelle. Im Übrigen werden die Protokolle ausschließlich zur Erkennung und Aufklärung von Sicherheits- und Datenschutzvorfällen, zur Erfüllung der Nachweis-, Auskunfts- und Rechenschaftspflichten der verantwortlichen Stelle sowie zur Rekonstruktion des Zustandekommens einer Ausgabe verwendet. Eine Verwendung zu anderen Zwecken ist unzulässig; der Ausschluss nach Abschnitt 10.1 Absatz 1 gilt für die Protokolldaten entsprechend, soweit die Lösung Funktionen nach Abschnitt 4.3 einsetzt.

(8) Setzt die Lösung Funktionen nach Abschnitt 4.3 ein, so hält der Auftragnehmer die Stände der dabei eingesetzten Modelle, Prompts und Konfigurationen so nachvollziehbar, dass sich zu einem erzeugten Vorschlag feststellen lässt, unter welchen Ständen er entstanden ist; die Angaben unterliegen den Anforderungen der Absätze 3 und 4.

7.2 Sicherheitsbezogene Überwachung, Security Monitoring

(1) Der Auftragnehmer beschreibt, welche sicherheitsrelevanten Ereignisse automatisiert überwacht werden, welche Schwellen eine Alarmierung auslösen, wer die Auswertung während welcher Zeiten vornimmt und in welcher Frist die Stelle, die den betroffenen Mandanten führt, und der Auftraggeber unterrichtet werden.

(2) Überwacht werden mindestens: gehäufte fehlgeschlagene Zugriffs- und Anmeldeversuche, auffällige Abfragemuster mit Rekonstruktionsverdacht, unerwartete administrative Zugriffe sowie

Abweichungen im Datenabfluss. Setzt die Lösung Funktionen nach Abschnitt 4.3 ein, werden zusätzlich die Erkennungen nach Abschnitt 8.3 Absatz 3 überwacht.

(3) Der Auftragnehmer setzt für die von ihm betriebene Lösung und deren Betriebsumgebung Systeme zur Angriffserkennung ein, die Merkmale aus dem laufenden Betrieb fortlaufend und automatisiert erfassen und auswerten. Erkennungsmuster und die hierfür eingesetzten Komponenten werden aktuell gehalten. Der Auftragnehmer beschreibt die eingesetzten Verfahren, deren Abdeckung sowie den Umgang mit erkannten Angriffsversuchen. Die Anforderung erstreckt sich nicht auf Netze, Systeme oder Endgeräte des Auftraggebers oder der Bedarfsträger. Die Anforderungen dieses Absatzes bilden die Grundanforderung Q-08 (Abschnitt 7.2 Absatz 3); sie ist unabhängig von einer gesetzlichen Betroffenheit als Betreiber einer kritischen Anlage vertragliche Muss-Leistung. Soweit der konkrete Einsatz zusätzlich in den Anwendungsbereich des § 31 Absatz 2 des BSI-Gesetzes fällt, dient sie zugleich der Erfüllung der dort geregelten Pflicht. Eine darüber hinausgehende Abdeckung wird nach dem Merkmal W-07 bewertet.

(4) Der Auftragnehmer stellt die Ereignisdaten eines Mandanten in einem auswertbaren Format der Stelle bereit, die diesen Mandanten führt. Umfang und Empfänger der Bereitstellung sind je Mandant konfigurierbar. Für Zwecke der Betriebssteuerung werden darüber hinaus aggregierte Angaben ohne Personenbezug bereitgestellt.

(5) Optionale Zusatzfunktion: Die Lösung ermöglicht die Anbindung an die Systeme zur Sicherheitsereignisverwaltung der Stellen, die die Mandanten führen. Sicherheitsrelevante Ereignisse werden hierfür über eine dokumentierte Schnittstelle in einem verbreiteten, strukturierten Format bereitgestellt, wahlweise fortlaufend oder in kurzen Abständen. Die Bereitstellung umfasst sämtliche Zugriffsebenen: fachliche Zugriffe der Nutzer, administrative und privilegierte Zugriffe, Zugriffe auf Schnittstellen, Zugriffe auf Datenhaltung sowie Such- und Indexdaten und, soweit vorhanden, Aufrufe der Funktionen nach Abschnitt 4.3. Die Ereignisse sind je Mandant getrennt abrufbar und enthalten die Angaben nach Abschnitt 7.1. Der Auftragnehmer beschreibt Format, Übertragungsweg, Aufsetzpunkte und Grenzen der Anbindung.

(6) Erfasst werden ferner unerwartete Prozessstarts und Codeausführungen in Verarbeitungsumgebungen, Zugriffsversuche auf Metadatendienste und Infrastrukturendpunkte, ungewöhnliche Verwendung technischer Identitäten, Zugriffe aus unerwarteten Netz- oder Systemkontexten sowie Abweichungen vom freigegebenen Kommunikationsprofil. Einzelereignisse werden über Komponenten, Identitäten und Systeme hinweg zusammengeführt und im Zusammenhang bewertet.

8 Sicherer Betrieb, Änderungen und Resilienz

8.1 Test-, Schulungs- und Entwicklungsdaten

(1) 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. Es gilt das Schutzniveau der Produktivumgebung.

(2) Ohne Weisung nach Absatz 1 sind ausschließlich synthetische oder wirksam anonymisierte Daten zu verwenden. Eine Pseudonymisierung genügt nicht.

(3) Solange Umgebungen Echtdaten enthalten, unterliegen sie demselben Schutzniveau wie die Produktivumgebung, einschließlich Zugriffskontrolle, Verschlüsselung, Protokollierung und Netztrennung.

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

(5) Echtdaten im Sinne dieses Abschnitts sind die in den Mandanten geführten Inhalte der Managementsysteme. Die Entscheidung über ihren Einsatz nach Absatz 1 trifft die Stelle, die den betroffenen Mandanten führt, und dokumentiert sie. Für die Erprobung nach Abschnitt 4.6 werden ausschließlich synthetische Daten verwendet.

8.2 Personalsicherheit und Vertraulichkeit

(1) 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.

(2) 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 Komponenten der künstlichen Intelligenz geschult. Der Auftragnehmer weist die Durchführung auf Verlangen nach.

(3) 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.

(4) 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.

(5) 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.

8.3 Sichere Entwicklung, Schwachstellen und Lieferkette

(1) Der Auftragnehmer weist für sämtliche kundenspezifischen Entwicklungen und Konfigurationen ein dokumentiertes sicheres Entwicklungs- und Freigabeverfahren nach. Dieses umfasst mindestens Vier-Augen-Prinzip und Code Review, automatisierte Sicherheits- und Abhängigkeitsprüfungen, Prüfung auf im Quellcode eingebettete Zugangsdaten und Schlüssel, getrennte Umgebungen für Entwicklung, Test und Produktion, kontrollierte Auslieferung mit signierten Artefakten sowie ein Rückfallverfahren.

(2) Der Auftragnehmer betreibt ein Schwachstellenmanagement für sämtliche Bestandteile der Lösung einschließlich Drittkomponenten, Bibliotheken, Container, Betriebssysteme, Datenbanken und Schnittstellen; setzt die Lösung Funktionen nach Abschnitt 4.3 ein, auch die dafür eingesetzten Komponenten einschließlich der zur Anbindung von Modellen eingesetzten Vermittlungsschichten wie Modell-Gateways, Router und Bibliotheken. Er schlägt nach Kritikalität gestaffelte Behebungsfristen vor, die der Zustimmung des Auftraggebers bedürfen und Vertragsbestandteil werden. Schwachstellen, die als kritisch eingestuft sind oder für die eine aktive Ausnutzung bekannt ist, sind unverzüglich zu behandeln. Der Auftragnehmer unterrichtet den Auftraggeber und die betroffenen Bedarfsträger über die konkrete Betroffenheit, stellt bei nicht sofort möglicher Behebung eine Übergangsmaßnahme bereit und weist die Behebung nach.

(3) Setzt die Lösung Funktionen nach Abschnitt 4.3 ein, so berücksichtigt der Auftragnehmer bei Schwachstellenmanagement und Sicherheitsprüfungen auch Angriffsformen, die sich speziell gegen solche Funktionen und die zugehörigen Retrieval-Komponenten richten und die zum Zeitpunkt des Vertragsschlusses noch nicht bekannt sind. Er wertet hierfür einschlägige Veröffentlichungen des Bundesamts für Sicherheit in der Informationstechnik und anerkannter Fachgremien aus und passt Schutzmaßnahmen und Prüfklassen in dem im Rahmenvertrag geregelten Änderungs- und Freigabeverfahren an.

(4) Der Auftragnehmer stellt für die eingesetzte Software eine Stückliste in maschinenlesbarer Form bereit und aktualisiert sie bei jeder Auslieferung. Die Stückliste wird im Format CycloneDX ab Version 1.6 oder SPDX ab Version 2.3 in JSON bereitgestellt, je Auslieferung mit Prüfsumme und Signatur; sie weist mindestens Komponente, Version, Lieferant, Lizenz und Paketkoordinaten aus, und, soweit die Lösung Funktionen nach Abschnitt 4.3 einsetzt, für die dafür eingesetzten Modellkomponenten zusätzlich Modellname, Modellversion, Anbieter und Verarbeitungsregion. Setzt die Lösung solche Funktionen ein, so zählen zu den sicherheitskritischen Komponenten auch die Komponenten, die Modelle ausführen oder bereitstellen, die Verfahren zur Zerlegung von Text in Token, native Beschleunigungsbibliotheken, die Verfahren zum Laden und Serialisieren von Modellen sowie deren Abhängigkeiten. Ergänzend stellt er im Format CycloneDX ab Version 1.6 in JSON eine Stückliste des schnittstellenrelevanten kryptografischen Materials als Cryptography Bill of Materials bereit. Die Objekte werden dabei als kryptografische Bestandteile der Stückliste ausgewiesen und nicht als freier Text beschrieben. Die Stückliste weist je Objekt Bezeichnung, Verwendungszweck, betroffene Schnittstelle sowie, soweit einschlägig, ausstellende Stelle und Gültigkeitszeitraum aus, für Zertifikate zusätzlich Aussteller, Subjekt, Seriennummer oder ein vergleichbares Erkennungsmerkmal, Signatur- und Schlüsselverfahren einschließlich Schlüssellänge sowie Beginn und Ende der Gültigkeit. Das Format SPDX ist für diese Stückliste nicht zugelassen. Für beide Stücklisten gelten dieselben Bereitstellungspflichten. Die kryptografische Stückliste ist darüber hinaus bei jeder Änderung des ausgewiesenen Materials zu aktualisieren. Private Schlüssel, geheime Schlüsselwerte, Passwörter, Zugangsmerkmale oder sonstiges unmittelbar nutzbares Geheimnismaterial dürfen nicht Bestandteil der bereitgestellten Angaben sein.

(5) Der Auftragnehmer benennt für die eingesetzten Dritt- und Modellkomponenten den jeweiligen Unterstützungszeitraum, innerhalb dessen der Hersteller Sicherheitsaktualisierungen bereitstellt. Er zeigt dem Auftraggeber unverzüglich an, wenn eine eingesetzte Komponente aus der Unterstützung fällt oder der Unterstützungszeitraum verkürzt wird, und legt dar, wie er die Sicherheit der Lösung anschließend gewährleistet. Der Einsatz von Komponenten ohne Herstellerunterstützung bedarf der vorherigen Zustimmung des Auftraggebers.

(6) Vor produktiver Nutzung wird eine technische Sicherheitsprüfung der produktionsnahen Gesamtlösung durch einen vom Auftragnehmer unabhängigen Dritten durchgeführt. Gegenstand sind mindestens Webanwendung, Schnittstellen, Authentifizierung einschließlich der föderierten Anmeldung nach Abschnitt 4.2, Trennung der Mandanten, administrative Zugänge sowie auf die angebotene Lösung bezogene Prüffälle. Der Bericht wird dem Auftraggeber und auf Verlangen der Stelle vorgelegt, die den betroffenen Mandanten führt. Kritische Feststellungen sind vor Produktivsetzung zu beheben; hohe Feststellungen sind zu beheben oder mit dokumentierter Zustimmung der Stelle, in deren Verantwortungsbereich das verbleibende Risiko wirkt, ausdrücklich risikobehandelt. Die Nachprüfung ist Voraussetzung der Abnahme nach Abschnitt 4.5. Für die Frist der Produktivbereitstellung nach Abschnitt 4.5 gilt: Liegt bei Abruf ein aktueller Bericht über eine Prüfung nach den Sätzen 1 und 2 vor, die ein vom Auftragnehmer unabhängiger Dritter am Standardstand der angebotenen Lösung durchgeführt hat, beträgt die Frist zwei Wochen nach Abruf; andernfalls beträgt sie sechs Wochen nach Abruf, und die Prüfung nach Satz 1 ist innerhalb dieser Frist durchzuführen. Aktuell ist ein Bericht, wenn die Prüfung nicht länger als zwölf Monate zurückliegt (Absatz 7 Satz 1) und der geprüfte Stand seither nicht wesentlich geändert wurde (Absatz 7 Satz 2). Gegenstand der Prüfung sind auch gemeinsam genutzte Infrastrukturbestandteile, insbesondere Paket- und Artefaktablagen, Modell- und Containerregister, Zwischenspeicher, temporäre Speicherdienste sowie Build- und Auslieferungsstrecken.

(7) Die Prüfung nach Absatz 6 wird als vollständige Prüfung der produktionsnahen Gesamtlösung durch einen unabhängigen Dritten alle zwölf Monate wiederholt. Nach Übernahme einer wesentlichen Änderung der Lösung oder einer wesentlichen Änderung der Betriebsumgebung werden der geänderte Teil und seine Schnittstellen innerhalb von zwanzig Werktagen geprüft. Festgestellte Mängel werden innerhalb von zwanzig Werktagen nach ihrer Behebung nachgeprüft. Der Prüfer wird vom Auftraggeber bestätigt und spätestens alle drei Jahre gewechselt; der vollständige Prüfbericht wird dem Auftraggeber vorgelegt. Der Prüfumfang umfasst die Angriffsformen nach Absatz 3.

(8) Der Auftragnehmer legt dar, ob die angebotene Lösung ganz oder teilweise in den Anwendungsbereich der Cyberresilienz-Verordnung fällt, und begründet die Einordnung. Fällt sie darunter, weist er die Erfüllung der ab dem 11. September 2026 geltenden Meldepflichten nach und stellt die Erfüllung der ab dem 11. Dezember 2027 geltenden Herstellerpflichten bis zu diesem Datum sicher.

(9) Sind kundenspezifische oder sicherheitsrelevante Bestandteile der Lösung wesentlich mit Unterstützung von Systemen der künstlichen Intelligenz erzeugt worden, legt der Auftragnehmer Umfang, eingesetzte Werkzeuge und das angewandte Prüfverfahren offen. Erfasst sind Programmcode, sicherheitsrelevante Konfigurationen und Testfälle, die in die geschuldete Lösung eingegangen sind. Nicht erfasst sind übliche Hilfsmittel der Entwicklungsumgebung ohne wesentlichen Beitrag zum Ergebnis. Für die erfassten Bestandteile gelten dieselben Anforderungen an Codeprüfung, Testabdeckung und Freigabe wie für die übrigen Bestandteile.

(10) Identitäten produktiver Laufzeitkomponenten haben keine Schreibberechtigung auf Quellcodeverwaltung, Build- und Auslieferungskonfigurationen, Artefakt- und Modellablagen sowie sonstige Systeme der Softwarelieferkette. Umgekehrt erhalten Build- und Auslieferungskomponenten keine Zugangsmittel der Produktivumgebung, die für ihren Zweck nicht erforderlich sind. Abweichungen bedürfen einer dokumentierten Risikobewertung und der vorherigen Freigabe des Auftraggebers.

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 zentrale Leistung, 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) Als meldepflichtiger Vorfall gilt ausdrücklich auch die Ausgabe von Inhalten eines Mandanten im Kontext eines anderen Mandanten, unabhängig davon, ob ein Datenabfluss nach außen vorliegt.

(4) 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.

(5) 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.

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

(7) 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.

8.5 Verfügbarkeit, Sicherung und Notbetrieb

(1) Die Mindestverfügbarkeit der zentral betriebenen Komponenten beträgt 99,5 Prozent. Sie wird monatlich gemessen und bezieht sich auf die für den jeweiligen Mandanten geschuldeten Funktionen nach Abschnitt 4.2. Sind Funktionen, die auf Verfahren der künstlichen Intelligenz beruhen, nach Abschnitt 4.3 angeboten und für den betreffenden Mandanten aktiviert, so bilden sie eine zweite Leistungsgruppe und werden gesondert gemessen; sind sie nicht aktiviert, ist der Wert der ersten Leistungsgruppe maßgeblich. Der Wert gilt für die Servicezeiten nach Abschnitt 8.7 Absatz 2; für die übrige Zeit beträgt die Mindestverfügbarkeit 99,0 Prozent. Das Messverfahren ergibt sich verbindlich aus Absatz 1a; Bieterangabe ist ausschließlich der zugesagte Verfügbarkeitswert. Die zugesagten Verfügbarkeitswerte und das vorgegebene Messverfahren werden Vertragsbestandteil.

(1a) Für die Messung der Verfügbarkeit gilt: Die Verfügbarkeit ergibt sich als Messzeit abzüglich Ausfallzeit, geteilt durch die Messzeit, mal hundert; Messzeit ist die Summe der Minuten des jeweiligen Zeitraums nach Absatz 1 im Kalendermonat. Sie wird je Leistungsgruppe und je Mandant berechnet; für die Vertragsfolgen maßgeblich ist der niedrigere Wert der gemessenen Leistungsgruppen. Ist nur für eine Leistungsgruppe ein Verfügbarkeitswert berechenbar, so ist für die Vertragsfolgen allein dieser Wert maßgeblich; ist für keine ein Wert berechenbar, entstehen aus der Verfügbarkeitsmessung für diesen Kalendermonat keine Vertragsfolgen. Gemessen wird durch eine synthetische Transaktion von einem vom Auftraggeber benannten Messpunkt außerhalb des Netzes des Auftragnehmers gegen die für die Nutzer bereitgestellte Schnittstelle. Die Transaktion der ersten Leistungsgruppe bildet Anmeldung, Öffnen eines Objekts des Managementsystems oder eines Registers, Suche oder Filterung, Lesen und Bearbeiten eines Testobjekts sowie den Abruf einer Auswertung oder eines Berichts ab. Die Transaktion der zweiten Leistungsgruppe bildet den Aufruf einer für den Mandanten aktivierten Funktion nach Abschnitt 4.3 auf einem Testobjekt und die Entgegennahme ihres Ergebnisses ab; der Auftragnehmer benennt mit dem Angebot je angebotener Funktion den hierfür maßgeblichen Ablauf, und er wird im Einzelvertrag festgehalten. Sind mehrere Funktionen aktiviert, genügt eine Transaktion je Funktionsart; die Messung erfasst dieselben Schritte bei allen Mandanten. Das Messintervall beträgt sechzig Sekunden. Ein Ausfall beginnt mit der ersten von zwei aufeinanderfolgenden fehlgeschlagenen Messungen und endet mit der ersten wieder erfolgreichen Messung, unabhängig von Meldung oder Kenntnis des Auftragnehmers. Als Ausfall gilt auch, wenn die Fehlerrate fünf Prozent übersteigt. Ausfälle von weniger als fünf Minuten werden nicht angerechnet; eine Obergrenze je Einzelstörung besteht nicht. Ausgeschlossen sind abschließend angekündigte Wartung nach Absatz 5, höhere Gewalt mit Ausnahme von Arbeitskämpfen beim Auftragnehmer oder seinen Unterauftragnehmern sowie vom Auftraggeber oder von einem Bedarfsträger zu vertretende Ursachen; Ausfälle bei Unterauftragnehmern, Cloud- und Modellanbietern sowie unaufschiebbare Notfallmaßnahmen sind nicht ausgeschlossen. Ob der zugesagte Wert erreicht ist, wird anhand des ungerundeten Ergebnisses festgestellt; die kaufmännische Rundung auf zwei Nachkommastellen dient allein der Darstellung im Bericht. Ausfallminuten werden ungerundet summiert. Der Auftragnehmer berichtet monatlich bis zum zehnten Werktag des Folgemonats und stellt die Rohdaten der Messung auf Verlangen maschinenlesbar bereit.

(2) Die Wiederanlaufzeit beträgt höchstens acht Stunden, der maximal tolerierbare Datenverlust höchstens vier Stunden, jeweils kalendarisch. Die Wiederanlaufzeit bezeichnet die Zeit bis zur Wiederherstellung des Betriebs aus der Datensicherung nach einem Verlust der produktiven Umgebung; die Wiederherstellungszeit für eine Störung richtet sich unabhängig hiervon nach Abschnitt 8.7 Absatz 3, und bei einem Zusammentreffen gilt die kürzere Frist. Der Bieter kann kürzere Werte zusagen; sie werden Vertragsbestandteil. Die in den Mandanten geführten Inhalte der Managementsysteme werden

vollständig in die Datensicherung einbezogen; ebenso die für den Betrieb erforderlichen Einstellungen und Zuordnungen und, soweit die Lösung Funktionen nach Abschnitt 4.3 einsetzt, die eingesetzten Modell-, Prompt- und Konfigurationsstände, sodass ein funktionsfähiger Vorzustand wiederhergestellt werden kann. Mindestens ein Satz der Sicherungen wird so vorgehalten, dass er aus der produktiven Umgebung heraus nicht verändert oder gelöscht werden kann. Die Wiederherstellung wird mindestens einmal jährlich sowie nach wesentlichen Änderungen an der Lösung oder ihrer Betriebsumgebung vollständig getestet; das Ergebnis wird dokumentiert und dem Auftraggeber vorgelegt.

(2a) Sicherungen dienen ausschließlich der Wiederherstellung des Betriebs. Eine Nutzung für Fehleranalyse, Erprobung, Auswertung oder Weiterentwicklung ist ausgeschlossen. Wird eine Sicherung eingespielt, prüft der Auftragnehmer unverzüglich, ob dabei Bestände zurückgeführt wurden, die zwischenzeitlich zu löschen waren, und löscht diese erneut; die Prüfung und die Löschung werden dokumentiert.

(2b) Der Auftragnehmer legt ein Datensicherungskonzept vor. Es benennt je Datenart die Sicherungsart, den Sicherungsrhythmus, die Aufbewahrungsdauer, den Speicherort und das Verfahren der Vernichtung. Sicherungen werden getrennt von der produktiven Umgebung aufbewahrt; die Trennung kann räumlich oder logisch erfolgen und ist zu beschreiben.

(2c) Die Lesbarkeit und Vollständigkeit der Sicherungen wird in einem festgelegten Rhythmus, mindestens halbjährlich, stichprobenartig geprüft. Das Ergebnis wird dokumentiert und dem Auftraggeber auf Verlangen vorgelegt.

(3) Der Auftragnehmer beschreibt den Notbetrieb bei Ausfall einzelner Komponenten der Lösung, ihrer Betriebsumgebung oder einzelner Schnittstellen. Setzt die Lösung Funktionen nach Abschnitt 4.3 ein, so muss der Zugriff auf die Inhalte des Managementsystems auch bei deren Ausfall erhalten bleiben.

(4) Die Stelle, die einen Mandanten führt, kann die Funktionen nach Abschnitt 4.3 für ihren Mandanten kurzfristig deaktivieren, ohne dass der Zugriff auf die Inhalte des Managementsystems entfällt. Die Deaktivierung ist ohne Mitwirkung des Auftragnehmers auslösbar; die Voraussetzungen und die Wirkung beschreibt der Auftragnehmer.

(5) Geplante Wartungsarbeiten finden ausschließlich außerhalb der Servicezeiten nach Abschnitt 8.7 Absatz 2 statt; das Fenster wird mit dem Auftraggeber abgestimmt und ist mindestens fünf Werktage vorher anzukündigen. Auswirkungen auf die Verfügbarkeit sind vorab mitzuteilen. Während des Wartungsfensters und bis zum Abschluss der anschließenden Funktionsprüfung hält der Auftragnehmer eine erreichbare Ansprechstelle vor und stellt die Rückkehr auf den vorherigen Stand innerhalb von zwei Stunden ab Feststellung des Fehlschlags sicher. Unaufschiebbare Notfallmaßnahmen sind zulässig und unverzüglich anzuzeigen.

8.6 Beherrschung leistungserforderlicher technischer Abhängigkeiten

(1) Der Auftragnehmer stellt sicher, dass leistungserforderliche technische Abhängigkeiten so betrieben, erneuert, ersetzt oder angepasst werden, dass deren Ablauf, Änderung, Widerruf oder sonstiger vorhersehbarer Wegfall nicht zu einer Beeinträchtigung der vertragsgegenständlichen Leistung führt. Bei einem unvorhersehbaren Ausfall oder Wegfall ergreift er unverzüglich die erforderlichen

Maßnahmen zur Wiederherstellung; die Anforderungen an die Störungsbearbeitung nach Abschnitt 8.7 bleiben unberührt.

(2) Geplante Änderungen sowie Erneuerungen, Ablösungen oder Anpassungen nach Absatz 1, die sich technisch auf die vertragsgegenständliche Leistung auswirken und deren Fehlschlagen diese beeinträchtigen kann, erprobt der Auftragnehmer vor ihrer produktiven Wirksamkeit. Die Erprobung bildet die hierfür maßgeblichen Eigenschaften und Abhängigkeiten der Produktivumgebung ab. Nach Eintritt der produktiven Wirksamkeit verifiziert er die ordnungsgemäße Funktion.

(3) Das Verfahren, mit dem der Auftragnehmer die Absätze 1 und 2 erfüllt, bleibt ihm überlassen. Für kryptografisches Material beschreibt er es im Rahmen von Abschnitt 6.2 Absatz 5.

(4) Eine Beeinträchtigung, die auf den vom Auftragnehmer zu verantwortenden Ablauf, Ausfall oder Wegfall oder auf die fehlerhafte Änderung einer leistungserforderlichen technischen Abhängigkeit zurückzuführen ist, begründet keinen Ausschlusstatbestand im Sinne von Abschnitt 8.5 Absatz 1a.

(5) Betrifft eine Änderung, ein Ablauf oder ein sonstiger Wechsel nach Absatz 1 Schnittstellen zum Auftraggeber oder zu den Bedarfsträgern oder erfordert er Mitwirkungshandlungen des Auftraggebers, zeigt der Auftragnehmer dies mit einer Frist von mindestens dreißig Kalendertagen vor der produktiven Wirksamkeit an. Die Anzeige benennt Art und Umfang, den vorgesehenen Zeitpunkt, die betroffenen Schnittstellen und die erforderlichen Mitwirkungshandlungen. Weitergehende Anzeigepflichten, insbesondere nach Abschnitt 8.5 Absatz 5, bleiben unberührt; treffen mehrere Fristen zusammen, gilt die längste.

(6) Soweit eine Änderung einer Erprobung nach Absatz 2 unterliegt und eine eigene technische Erprobung durch den Auftraggeber erforderlich ist, stellt der Auftragnehmer diesem nach erfolgreicher eigener Erprobung eine geeignete Erprobungsmöglichkeit bereit, die die für die Änderung maßgeblichen Eigenschaften und Abhängigkeiten abbildet, und benennt hierfür einen Zeitraum von mindestens zehn Werktagen vor der produktiven Wirksamkeit. Die eigene Erprobung durch den Auftraggeber ist ein Recht und keine Pflicht; aus ihrer Nichtwahrnehmung kann der Auftragnehmer keine Rechte herleiten, und seine Verantwortung nach den Absätzen 1 und 2 bleibt unberührt.

(7) Ist eine Änderung oder ein Wechsel aus Sicherheitsgründen unaufschiebbar, entfallen die Fristen nach den Absätzen 5 und 6, soweit ihre Einhaltung aufgrund der Dringlichkeit nicht möglich ist. Die Anzeige erfolgt unverzüglich, spätestens mit Eintritt der produktiven Wirksamkeit, und wird begründet. Auch in diesem Fall hält der Auftragnehmer eine Rückfallmöglichkeit auf den vorherigen Stand vor oder beschreibt, warum eine solche technisch nicht besteht und mit welchen Maßnahmen er die Leistung bei einem Fehlschlagen der Änderung wiederherstellt; dies gilt insbesondere für Abhängigkeiten von Modellschnittstellen, Identitätsdiensten und Zertifikaten. Die Pflichten nach Abschnitt 8.7 bleiben unberührt.

8.7 Störungsbearbeitung und Erreichbarkeit

(1) Anfragen zu Störungen und Serviceanliegen werden über mindestens zwei Wege entgegengenommen. Bereitzustellen sind mindestens eine zentrale E-Mail-Adresse sowie ein Ticketsystem oder eine Weboberfläche zur Eröffnung von Supportfällen. Jede Anforderung erhält eine Fallnummer; der Bearbeitungsstatus ist nachvollziehbar. Der Support erfolgt in deutscher Sprache aus dem Europäischen

Wirtschaftsraum, für den ersten und zweiten Bearbeitungsgrad mindestens auf dem Niveau C1 oder vergleichbar.

(2) Die Servicezeiten umfassen mindestens Montag bis Freitag, von 08:00 bis 17:00 Uhr, jeweils ausgenommen bundeseinheitliche Feiertage, sofern keine abweichenden Servicezeiten vereinbart werden.

(3) Für Störungen gelten drei Klassen. Den Betrieb verhindernd ist eine Störung, bei der die Lösung oder eine Leistungsgruppe nach Abschnitt 8.5 Absatz 1 nicht nutzbar ist; den Betrieb behindernd ist eine Störung, bei der wesentliche Funktionen nur eingeschränkt nutzbar sind; leicht ist jede sonstige Störung. Die Einstufung nimmt der Auftraggeber im Benehmen mit dem betroffenen Bedarfsträger vor; widerspricht der Auftragnehmer, laufen die Fristen weiter. Bei einer den Betrieb verhindernden Störung beträgt die Reaktionszeit eine Stunde und die Wiederherstellungszeit fünf Stunden. Bei einer den Betrieb behindernden Störung beträgt die Reaktionszeit zwei Stunden und die Wiederherstellungszeit zwei Werktage. Bei einer leichten Störung beträgt die Reaktionszeit einen Werktag und die Wiederherstellungszeit fünf Werktage. Für Serviceanfragen ohne Störung beträgt die Reaktionszeit einen Werktag und die Erledigungszeit zehn Werktage. Reaktion ist eine qualifizierte Rückmeldung mit Einschätzung der Ursache und, soweit möglich, einer Umgehung; eine automatische Eingangsbestätigung genügt nicht. Bei den Betrieb behindernden und leichten Störungen beendet eine tragfähige Umgehungslösung die Wiederherstellungsfrist; die endgültige Behebung folgt mit der nächsten planmäßigen Auslieferung. Verfehlt der Auftragnehmer die Reaktions- oder Wiederherstellungszeit, erhält der betroffene Bedarfsträger eine Nichterfüllungsgutschrift auf die monatliche Betriebsvergütung des Einzelvertrags. Sie beträgt bei einer den Betrieb verhindernden Störung fünf Prozent je angefangene weitere Stunde und bei einer den Betrieb behindernden Störung zwei Prozent je angefangenen weiteren Arbeitstag, insgesamt höchstens zwanzig Prozent im Kalendermonat. Erreicht die nach Abschnitt 8.5 für die Vertragsfolgen maßgebliche Verfügbarkeit den zugesagten Wert im Kalendermonat nicht, beträgt die Gutschrift fünf Prozent der monatlichen Vergütung des Einzelvertrags für die erste angefangene Zehntelstufe unterhalb des zugesagten Wertes, zehn Prozent ab der zweiten und fünfzehn Prozent ab der fünften, insgesamt höchstens dreißig Prozent im Kalendermonat. Monatliche Vergütung des Einzelvertrags ist die Summe der für den Kalendermonat geschuldeten laufenden Betriebsvergütung und der für den Kalendermonat abgerechneten leistungsabhängigen Vergütung. Einmalige und gesondert abgerufene Entgelte bleiben außer Betracht, insbesondere Entgelte für Änderungen und für Erweiterungen nach Abschnitt 4.9 (Position 8 der Anlage 07.3) sowie nach Tagessätzen abgerechnete Leistungen (Positionen 5 bis 7 der Anlage 07.3); andernfalls hinge die Gutschrift von zufälligen Abrechnungen desselben Kalendermonats ab. Eine Aufteilung dieses Betrages auf die Leistungsgruppen findet nicht statt. Die Unterschreitung des zugesagten Wertes in beiden Leistungsgruppen führt nicht zu einer doppelten Verfügbarkeitsgutschrift; maßgeblich ist nach Abschnitt 8.5 Absatz 1a der niedrigere Verfügbarkeitswert und damit die höhere Gutschrift. Die Gutschriften sind pauschalierter Ausgleich. Weitergehende Ansprüche, insbesondere auf Minderung, Schadensersatz und Kündigung, bleiben unberührt; dem Auftragnehmer bleibt der Nachweis eines geringeren Schadens offen. Vertragsstrafen für die Nichteinhaltung der Reaktions- und Wiederherstellungszeiten und für die Nichteinhaltung der zugesagten Verfügbarkeit werden nicht vereinbart; die Nummern 17.2 und 17.3 des Einzelvertrags (Anlage 31.0) bleiben ohne Eintrag. Die Vertragsstrafe bei Verzug nach den EVB-IT System-AGB bleibt unberührt. Die Gutschriften werden auf einen Anspruch auf Minderung und auf Schadensersatz angerechnet.

(4) Die Zeiten nach Absatz 3 laufen innerhalb der Servicezeiten; abweichend hiervon laufen die Reaktionszeit von einer Stunde und die Wiederherstellungszeit von fünf Stunden bei einer den Betrieb

verhindernden Störung kalendarisch rund um die Uhr an allen Tagen des Jahres. Erfasst die Messung nach Abschnitt 8.5 Absatz 1a die Störung, so beginnen die Reaktions- und Wiederherstellungszeiten mit dem Beginn des Ausfalls nach jener Bestimmung; auf die Kenntnis des Auftragnehmers kommt es insoweit nicht an. Im Übrigen beginnen sie mit dem Eingang der Störungsmeldung oder, wenn der Auftragnehmer die Störung zuvor selbst feststellt, mit seiner Kenntnis. Die Begriffsbestimmungen der EVB-IT System-AGB, nach denen die Reaktionszeit mit dem Zugang der Störungsmeldung innerhalb der vereinbarten Servicezeiten beginnt und die Reaktions- und die Wiederherstellungszeit ausschließlich während der vereinbarten Servicezeiten laufen, gelten nicht, soweit dieser Absatz Beginn und Lauf der Zeiten abweichend regelt.

(5) Eine den Betrieb verhindernde Störung teilt der Auftragnehmer dem betroffenen Bedarfsträger und dem Auftraggeber ab eigener Kenntnis mit, ohne dass es einer vorherigen Meldung bedarf; die Frist beträgt vier Stunden. Die Mitteilung enthält die zu diesem Zeitpunkt bekannten Auswirkungen und Handlungsempfehlungen; noch fehlende Erkenntnisse sind als solche zu benennen und nachzureichen. Die Mitteilungspflicht besteht unabhängig davon, ob zugleich ein Vorfall nach Abschnitt 8.4 vorliegt.

(6) Der Auftragnehmer benennt eine Kontaktstelle, die für Meldungen und Abstimmungen nach Abschnitt 8.4 durchgängig erreichbar ist, an allen Tagen des Jahres und unabhängig von den vereinbarten Servicezeiten. Da die Reaktions- und Wiederherstellungszeiten für eine solche Störung nach Absatz 4 kalendarisch laufen, hält der Auftragnehmer auch außerhalb der Servicezeiten die technische Eingriffs- und Wiederherstellungsfähigkeit vor, die zur Einhaltung dieser Zeiten erforderlich ist; eine Stelle, die eine Meldung lediglich entgegennimmt und weiterleitet, genügt hierfür nicht. Der Meldeweg zu dieser Kontaktstelle muss von der betroffenen Leistung technisch unabhängig sein und auch bei deren vollständigem Ausfall zur Verfügung stehen. Die Melde- und Berichtsfristen nach Abschnitt 8.4 laufen kalendarisch und werden durch die vereinbarten Servicezeiten nicht gehemmt. Die Mitteilungsfrist nach Absatz 5 läuft ausschließlich innerhalb der Servicezeiten nach Absatz 2. Der Auftragnehmer weist Erreichbarkeit und Meldeweg vor Produktivsetzung nach.

(7) Der Auftragnehmer benennt namentlich eine für den Betrieb verantwortliche Ansprechperson sowie deren Vertretung. Ein Wechsel wird dem Auftraggeber unverzüglich angezeigt.

(8) Auftraggeber und Auftragnehmer führen mindestens einmal je Quartal ein Regelgespräch zum Betrieb. Der Auftragnehmer legt hierzu einen Bericht vor, der mindestens die Verfügbarkeit, die Antwortzeiten, die Zahl und Bearbeitungsdauer der Störungen und Serviceanfragen nach Klassen sowie die Einhaltung der vereinbarten Werte ausweist. Werden vereinbarte Werte nicht erreicht, benennt der Auftragnehmer die Ursachen und die vorgesehenen Maßnahmen und weist deren Wirkung im folgenden Bericht nach.

9 Prüfrechte und Vertragsende

9.1 Prüfrechte, wiederkehrende Überprüfung und Betriebsdokumentation

(1) Der Auftraggeber oder ein von ihm beauftragter Dritter kann die Einhaltung der Anforderungen der Kapitel 5 bis 10 mindestens einmal jährlich sowie anlassbezogen prüfen, dokumentenbasiert und vor Ort. Das Prüfrecht erstreckt sich auf Unterauftragnehmer; der Auftragnehmer stellt dies vertraglich

sicher. Die Rechte der jeweils verantwortlichen Stelle aus dem Vertrag über die Auftragsverarbeitung bleiben unberührt; Einzelheiten zur Ausübung durch einen Bedarfsträger und zur Bündelung mehrerer Prüfungen regeln die Rahmenvereinbarung und der Einzelvertrag.

(2) Der Auftragnehmer duldet technische Sicherheitsprüfungen einschließlich Penetrationstests, die der Auftraggeber selbst oder durch einen von ihm Beauftragten durchführen lässt, und wirkt daran mit. Er stellt hierfür eine geeignete Umgebung, die erforderlichen Zugänge und eine Ansprechperson bereit. Prüfumfang, Prüfziele und Prüfzeitfenster werden vorher in Textform abgestimmt. Werden Komponenten Dritter berührt, holt der Auftragnehmer deren Zustimmung ein und teilt dem Auftraggeber unverzüglich mit, wenn und in welchem Umfang sie nicht erteilt wird. Feststellungen werden nach Abschnitt 8.3 behandelt; die Mitwirkung wird nicht gesondert vergütet.

(3) Der Auftragnehmer überprüft mindestens einmal jährlich die Wirksamkeit seiner Sicherheitsmaßnahmen und derjenigen seiner Unterauftragnehmer und berichtet dem Auftraggeber über Ergebnis und abgeleitete Maßnahmen.

(4) Zertifikate und Prüfnachweise für die Betriebsumgebung sind bei Ablauf, bei Änderung des Geltungsbereichs oder bei wesentlichen Feststellungen unaufgefordert zu aktualisieren. Der Auftragnehmer weist mindestens einmal jährlich nach, dass die von ihm beauftragten Unterauftragnehmer, Modellanbieter sowie Infrastruktur- und Plattformdienstleister die Anforderungen der Kapitel 5 bis 10 weiterhin erfüllen; dies umfasst deren aktuelle Zertifikate oder Testate mit Geltungsbereich und Prüfzeitraum.

(5) Der Auftragnehmer führt eine Betriebs- und Sicherheitsdokumentation der von ihm verantworteten Komponenten fort und übergibt sie bei wesentlichen Änderungen aktualisiert an den Auftraggeber.

(6) 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.

(7) Nach einem Sicherheitsvorfall leitet der Auftragnehmer dokumentierte Verbesserungsmaßnahmen ab und weist deren Umsetzung nach.

9.2 Datenrückgabe, Löschung und technische Übergabe bei Vertragsende

(1) Der Auftragnehmer weist die vollständige Löschung oder Rückgabe aller Daten nach, einschließlich der Bestände bei Unterauftragnehmern, in Sicherungen und, soweit die Lösung Funktionen nach Abschnitt 4.3 einsetzt, bei Modellanbietern; die Rückgabe erfolgt in einem strukturierten, gängigen und maschinenlesbaren Format nach Maßgabe der Verordnung (EU) 2023/2854. Der Nachweis erfolgt schriftlich und je beteiligter Stelle. Der Auftragnehmer weist den Lösch- und Überschreibungszyklus seiner Datensicherungen aus.

(2) Administrative Zugänge, Schnittstellenkonten, Zertifikate und Schlüssel werden nach einem abgestimmten Plan deaktiviert beziehungsweise widerrufen; die Durchführung wird bestätigt.

(3) Übergeben werden die Schnittstellendokumentation, kundenspezifische Mappings und Konfigurationsstände nach Maßgabe des Abschnitts 11.4 in verwertbarer Form; setzt die Lösung Funktionen nach Abschnitt 4.3 ein, auch die verwendeten Prompt- und Regelkonfigurationen. Zusätzlich übergeben werden die Anforderungs- und Maßnahmenkataloge, Bausteine, Bewertungsmaßstäbe, Klassifizierungsschemata, Objektarten und Vorlagen des jeweiligen Mandanten nach Abschnitt 4.2. Daten und Ergebnisse werden in offenen, dokumentierten oder allgemein verbreiteten Formaten übergeben, die ohne Werkzeuge des Auftragnehmers und ohne Verlust der inhaltlichen Struktur weiterverarbeitet werden können. Der Auftragnehmer benennt die Formate mit dem Angebot und beschreibt, welche Inhalte bei einer Übernahme in eine andere Lösung nicht verlustfrei überführbar sind.

(3a) Soll die Lösung zu einem anderen Betreiber überführt werden, übergibt der Auftragnehmer die für Dimensionierung, Migration und Wiederaufnahme erforderlichen Betriebs-, Plattform- und Konfigurationsunterlagen. Dazu gehören eine Aufstellung der eingesetzten Plattformkomponenten mit ihren Anforderungen, die über die letzten zwölf Monate erhobenen Werte zu Auslastung und Leistungsbedarf sowie eine Beschreibung der virtuellen Systeme und ihrer Konfiguration. Dazu gehört ferner eine Aufstellung der leistungserforderlichen technischen Abhängigkeiten nach Abschnitt 8.6, insbesondere der genutzten Modell- und Plattformdienste mit ihren Schnittstellen, der externen Schlüssel- und Zertifikatsverwaltungen und etwaiger herstellergebundener Laufzeitkomponenten, jeweils mit der Angabe, ob und unter welchen Voraussetzungen sie bei einem anderen Betreiber fortgeführt werden können. Standardbestandteile und Rechte Dritter bleiben unberührt; Abschnitt 11.4 geht vor. Der Auftragnehmer benennt mit dem Angebot, in welcher Form er diese Unterlagen bereitstellt.

(4) Die in einem Mandanten geführten Inhalte werden nach Weisung der Stelle, die diesen Mandanten führt, exportiert oder gelöscht. Die Weisung richtet sich nach dem für diese Inhalte festgelegten aktenrechtlichen Status.

(5) Die Dokumentationspflicht bei Vertragsende beschränkt sich auf die für Betrieb, Sicherheit, Migration und Nachweisführung relevanten Komponenten.

(5a) Setzt die Lösung Funktionen nach Abschnitt 4.3 ein, so werden die nach Abschnitt 7.1 Absatz 8 vorgehaltenen Stände bei Vertragsende in einer Form übergeben, die ihre Auflösung ohne Mitwirkung des Auftragnehmers erlaubt. Die Nutzungsrechte nach Abschnitt 11.4 bleiben unberührt.

(6) Für den Fall, dass der Auftragnehmer die Leistung aus rechtlichen oder wirtschaftlichen Gründen dauerhaft nicht mehr erbringen kann, beschreibt er, wie der Zugriff des Auftraggebers und der Bedarfsträger auf ihre Daten sowie eine geordnete Überführung sichergestellt werden. Er benennt die hierfür erforderlichen Unterlagen, Konfigurationen und Zugangsmittel und hält sie in einer Form vor, die dem Auftraggeber im Bedarfsfall zur Verfügung steht.

(7) Die Verpflichtungen dieses Abschnitts gelten auch, wenn ein einzelner Mandant die Nutzung beendet oder zu einem anderen Auftragnehmer wechselt, ohne dass der Rahmenvertrag endet. In diesem Fall sind Löschung, Rückgabe und Übergabe für die Inhalte dieses Mandanten gesondert nachzuweisen.

Die Stelle, die einen Mandanten führt, kann die Nutzung einzelner Funktionen nach Abschnitt 4.3 für ihren Mandanten einstellen, ohne den Vertrag zu beenden. In diesem Fall baut der Auftragnehmer die zugehörigen Verarbeitungsbestände geordnet ab, insbesondere Indizes, Einbettungen, zwischengespeicherte Kontexte und Modellzugänge, und weist dies nach. Die übrigen Leistungen bleiben unberührt. Der Auftragnehmer beschreibt das Verfahren, die erforderliche Vorlaufzeit und die Auswirkungen auf die verbleibenden Funktionen. Die Abschaltbarkeit je Mandant nach Abschnitt 4.3 bleibt unberührt und geht vor.

10 Einsatz von Komponenten der künstlichen Intelligenz

10.1 Grundsätze für den Einsatz

Dieses Kapitel gilt, soweit die Lösung Funktionen enthält, die auf Verfahren der künstlichen Intelligenz beruhen. Enthält sie keine solchen Funktionen, entfallen seine Anforderungen; Abschnitt 4.3 bleibt unberührt und geht vor.

(1) Eine Nutzung von Eingabe-, Kontext-, Dokument-, Metadaten-, Chat- oder Ergebnisdaten zu Zwecken des Trainings, des Fine-Tunings, des Reinforcement Learning, der Evaluierung, des Benchmarking, der Missbrauchserkennung außerhalb des konkreten Verarbeitungsvorgangs oder der Produktverbesserung ist ausgeschlossen. Der Ausschluss erfasst die Speicherung von Prompts und Antworten beim Modellanbieter sowie jede menschliche Einsichtnahme auf Seiten des Auftragnehmers, seiner Unterauftragnehmer und der Modellanbieter. Der Ausschluss der Nutzung zu Trainings- und Weiterentwicklungszwecken nach Abschnitt 4.3 bleibt unberührt.

(1a) Der Auftragnehmer darf die zur Leistungserbringung eingesetzte Infrastruktur auch für eigene Zwecke nutzen, insbesondere für eigene Trainings-, Erprobungs- und Entwicklungsläufe, soweit sämtliche nachstehenden Voraussetzungen erfüllt sind: Solche Läufe greifen weder unmittelbar noch mittelbar auf Daten der Bedarfsträger zu und verarbeiten keine hieraus abgeleiteten Zwischenergebnisse, Einbettungen, Indizes oder Modellstände; die Mandantentrennung nach den Abschnitten 4.2 und 6.1 wird auch ihnen gegenüber technisch durchgesetzt und auf Verlangen nachgewiesen; die Vertraulichkeit und die Integrität der Verarbeitung werden nicht beeinträchtigt; und die zugesagten Werte zur Verfügbarkeit nach Abschnitt 8.5 sowie zu den Reaktions- und Wiederherstellungszeiten nach Abschnitt 8.7 werden auch bei gleichzeitiger Eigennutzung eingehalten. Der Auftragnehmer legt mit dem Angebot offen, ob und in welchem Umfang er die Infrastruktur in dieser Weise mitnutzt, auf welchen Ebenen die Trennung wirkt und mit welchen Mitteln er die Einhaltung der Leistungszusagen bei gleichzeitiger Eigennutzung sicherstellt. Eine Verlagerung von Rechen- oder Speicherressourcen zwischen solchen Läufen und der produktiven Verarbeitung ist nur zulässig, soweit sie diese Voraussetzungen wahrt; sie wird nach Abschnitt 7.1 protokolliert. Weist der Auftragnehmer die Trennung für eine Komponente nicht nach, ist die Mitnutzung für diese Komponente unzulässig. Nutzt der Auftragnehmer die Infrastruktur in dieser Weise mit, so weist er auf Verlangen nach, dass die Voraussetzungen auch bei gleichzeitiger Eigennutzung eingehalten werden.

(2) An eine Komponente der künstlichen Intelligenz werden ausschließlich diejenigen Daten übergeben, die für den jeweiligen Verarbeitungsvorgang erforderlich sind. Eine vollständige Übergabe der gesamten Inhalte des Managementsystems darf nicht erforderlich sein. Der Auftragnehmer beschreibt, nach welchem Verfahren die für eine Anfrage erforderlichen Inhalte ausgewählt werden, und

weist nach, dass nicht erforderliche Inhalte nicht übergeben werden. Das Zustimmungserfordernis des Abschnitts 4.3 für die Übergabe von Risikobeurteilungen, Auditfeststellungen und Schwachstellen bleibt unberührt und geht vor.

(3) System- und Aufgabenprompts werden zentral verwaltet; Änderungen sind versioniert und nachvollziehbar dokumentiert. In Prompts werden keine personenbezogenen Daten, Zugangsdaten oder sonstigen schützenswerten Inhalte hinterlegt. Prompts werden nicht zur Durchsetzung von Berechtigungen oder Rollentrennungen eingesetzt; die Zugriffskontrolle erfolgt ausschließlich nach Abschnitt 6.1 und nach dem Rollenkonzept des Abschnitts 4.2.

(4) Automatische Aktualisierungen von Komponenten der künstlichen Intelligenz in der Produktivumgebung ohne vorherige Freigabe des Auftraggebers sind unzulässig. Die Lösung nutzt ausschließlich versionsfest gebundene Modellstände; ein Wechsel des Modellstands durch den Modellanbieter wirkt sich erst nach Freigabe durch den Auftraggeber auf die Produktivumgebung aus. Hiervon unberührt bleiben Sicherheits- und Plattformaktualisierungen der Betriebsumgebung, die das Verhalten dieser Komponenten nicht verändern; sie erfolgen nach Abschnitt 8.5 Absatz 5.

(5) Der Auftragnehmer beschreibt die Absicherung seiner Softwarelieferkette einschließlich Bezugsquellen, Signaturprüfung und Freigabeverfahren. Modelle und Modellartefakte werden ausschließlich aus nachvollziehbar vertrauenswürdigen Quellen bezogen; vorhandene Signaturen und Prüfsummen werden vor der Verwendung geprüft. Es werden Dateiformate verwendet, bei denen das Laden keine Ausführung von Programmcode auslöst; als unsicher geltende Formate werden nicht eingesetzt. Der Auftragnehmer benennt die verwendeten Formate und Prüfverfahren.

(6) Für automatisiert ablaufende Verarbeitungsketten besteht ein dokumentierter Abbruchmechanismus, der ohne Neustart der Gesamtlösung wirksam wird. Auslösebedingungen, Zuständigkeit und Wiederanlaufverfahren sind im Betriebshandbuch beschrieben. Nach dem Abbruch werden keine weiteren Werkzeug- oder Schnittstellenaufrufe ausgeführt; bereits begonnene Aktionen werden beendet oder zurückgesetzt, ohne dass Datenbestände in einem widersprüchlichen Zustand verbleiben. Die Wirksamkeit wird im Rahmen der Abnahme nach Abschnitt 4.5 nachgewiesen.

(7) Setzt die Lösung Komponenten ein, die ohne unmittelbare Auslösung durch eine Person Werkzeuge, Schnittstellen oder Fremdsysteme aufrufen, gilt ergänzend: Jede solche Komponente verfügt über eine eigene technische Identität; persönliche Zugangsdaten werden nicht weitergegeben oder wiederverwendet. Ist die Verarbeitung einer auslösenden Person zuzuordnen, wird deren Nutzer-, Rollen- und Mandantenkontext für die Autorisierung übernommen; die Komponente erhält keine weiter gehenden Rechte als diese Person. Für Verarbeitungen ohne auslösende Person, insbesondere zeit- oder ereignisgesteuerte Läufe, Wiederholungsversuche und Nachbearbeitungen, gilt ein für den jeweiligen Prozess festgelegtes technisches Berechtigungsprofil, das auf die erforderlichen Mindestrechte beschränkt und auf die betroffenen Mandanten begrenzt ist; der Auftragnehmer beschreibt diese Profile und lässt sie vom Auftraggeber freigeben. Der aufrufbare Umfang an Werkzeugen und Zielsystemen ist ausdrücklich festgelegt und technisch begrenzt. Aufrufkette, aufgerufenes Werkzeug, Zielsystem, ausgeführte Aktion, verwendete technische Identität, Berechtigungsentscheidung sowie Status- und Fehlerangaben werden nach Abschnitt 7.1 protokolliert; vollständige Eingabe- und Ausgabeinhalte werden nicht protokolliert. Der Inhaltsbezug erfolgt über Kennungen und Fundstellenverweise.

(8) Der Auftragnehmer erklärt mit dem Angebot, ob die Lösung solche Komponenten enthält, und beschreibt sie in einer Komponentenübersicht.

(9) Jeder Werkzeug-, Schnittstellen- oder Fremdsystemaufruf wird vor der Berechtigungsentscheidung gegen ein abgeschlossenes, versioniertes und für den jeweiligen Verarbeitungszusammenhang freigegebenes Verzeichnis aufgelöst. Nicht vorhandene, nicht eindeutig auflösbare, abgeschaltete oder nicht freigegebene Werkzeuge und Operationen werden abgelehnt. Die Auflösung stützt sich nicht allein auf die Bezeichnung des Werkzeugs, sondern zusätzlich auf Betreiber, Namensraum, Versionsstand und das vereinbarte Format der Ein- und Ausgaben; gleichlautende Bezeichnungen führen nicht zu einer automatischen Zuordnung. Übergebene Parameter werden vollständig gegen das freigegebene Format geprüft; unbekannte Parameter, nicht vereinbarte Felder und unzulässige Umwandlungen werden abgelehnt. Eine selbsttätige Ergänzung oder Korrektur sicherheitsrelevanter Parameter erfolgt nicht.

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

Soweit die Leistungserbringung im Einzelfall Sozialdaten im Sinne des § 35 des Ersten Buches Sozialgesetzbuch oder Gesundheitsdaten im Sinne des Artikels 9 der Verordnung (EU) 2016/679 berührt, sind die hierfür geltenden Vorgaben, insbesondere die §§ 67 ff. des Zehnten Buches Sozialgesetzbuch, einzuhalten.

Der Auftragnehmer verarbeitet grundsätzlich keine Sozial- oder Gesundheitsdaten. Die Lösung ist kein Ablageort für operative Sozial- oder Gesundheitsdaten; solche Daten werden dort weder gespeichert noch zur Bearbeitung vorgehalten.

Werden im Einzelfall dennoch Sozial- oder Gesundheitsdaten verarbeitet, so gelten die Kapitel 5 bis 10 und zusätzlich: Die Verarbeitung erfolgt ausschließlich auf dokumentierte Weisung der verantwortlichen Stelle und nur zu dem von ihr bestimmten Zweck; die abrufende Stelle schließt hierfür eine eigene Vereinbarung zur Auftragsverarbeitung nach Artikel 28 der Verordnung (EU) 2016/679 und § 80 des Zehnten Buches Sozialgesetzbuch; die Verarbeitung ist auf den erforderlichen Umfang und auf die hierfür benannten Personen beschränkt und wird dokumentiert; sie wird nach Wegfall des Zwecks beendet und die Daten werden nachweisbar gelöscht.

Unberührt bleiben in jedem Fall die Anforderungen zu Verschwiegenheit, Schulung und Personalsicherheit nach den Abschnitten 8.2 und 11.2.

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. Soweit hierfür ein Zugang zu Systemen des Auftraggebers oder eines Bedarfsträgers erforderlich ist, stellt der Auftraggeber oder, bei einem eigenen Abruf, der abrufende Bedarfsträger einen gesicherten Fernzugang bereit; die Anforderungen des Abschnitts 6.6 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 weder als Aufwand in Personentagen abgerechnet noch auf eine Höchstabrufmenge angerechnet. 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 Rechte an Arbeitsergebnissen

Der Auftragnehmer übergibt die für die jeweils abrufende Stelle erstellten Arbeitsergebnisse in bearbeitbarer und, soweit maschinelle Weiterverarbeitung in Betracht kommt, in strukturierter und maschinenlesbarer Form. Die abrufende Stelle erhält daran ein einfaches, zeitlich, räumlich und inhaltlich unbeschränktes, übertragbares Nutzungsrecht einschließlich des Rechts zur Weitergabe an die Bedarfsträger und an einen Nachfolgeauftragnehmer.

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.