Anlage A09 zum Vergabeverfahren 0311-2026

EVIGAIN - Leistungsbeschreibung Cloudleistungen, KI-Modelle und Schnittstellen

Kapitelbaustein für die Ausschreibung zur fachlichen Konzeption und technischen Umsetzung einer KI-basierten Versorgungslösung für nichtübertragbare Erkrankungen

Kapitel X - Anforderungen an Cloudleistungen, KI-Modelle und Schnittstellen

1. Gegenstand

In diesem Dokument werden die konkreten Anforderungen an die Teilleistungen Clouddienste, KI-Modelle und Schnittstellen beschrieben, die als verbindlicher Bestandteil des Leistungsumfangs gelten. Diese Anforderungen sind, wie in der Anlage A10 Bieterkonzept beschrieben, im Rahmen der Erstellung des einzureichenden Teilkonzeptes 3 – Cloud-, Sicherheits- und Datenschutzkonzept zu berücksichtigen.

Die Anforderungen betreffen sämtliche Cloud- und Hosting-Komponenten, Plattformen, Infrastrukturdienste, KI-Dienste, Modellinferenzdienste, Administrationsumgebungen, Monitoring- und Logging-Systeme, Backup- und Wiederherstellungssysteme sowie sonstige Dienste, die im Zusammenhang mit der Leistungserbringung eingesetzt werden oder auf personenbezogene Daten, sensible Gesundheitsdaten, Metadaten, Konfigurationsdaten oder sicherheitsrelevante Systeminformationen zugreifen können.

Die nachstehenden Anforderungen sind vom Auftragnehmer während der gesamten Vertragslaufzeit einzuhalten. Soweit der Auftragnehmer zur Leistungserbringung Leistungen Dritter einsetzt, hat er sicherzustellen, dass diese Anforderungen auch von den eingesetzten Cloud-Anbietern, Modellanbietern und Unterauftragnehmern erfüllt werden.

2. Allgemeine Anforderungen an die Cloud- und KI-Umgebung

Die angebotene Lösung ist in einer Cloud- und Betriebsumgebung zu betreiben, die in technischer, organisatorischer, datenschutzrechtlicher und informationssicherheitsbezogener Hinsicht für die Verarbeitung personenbezogener und sensibler Gesundheitsdaten geeignet ist. Dies bedeutet, dass die für Leistungen dieser Art relevanten Vorgaben der Gesetze SGB V, Digitalen Gesundheitsanwendungen-Verordnung oder Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG) zu erfüllen sind, insbesondere im Bereich der C5-Kriterien.

Die Cloud- und KI-Umgebung muss so ausgestaltet sein, dass Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Daten gewährleistet sind, eine klare Trennung zwischen Entwicklungs-, Test-, Evaluations- und Produktivumgebungen besteht, unbefugte Zugriffe ausgeschlossen oder auf das notwendige Minimum reduziert werden und sämtliche sicherheits- und datenschutzrelevanten Zugriffe nachvollziehbar dokumentiert werden.

Die angebotene Lösung muss nachvollziehbar, dokumentiert und auditierbar sein. Nicht dokumentierte Sonderkonfigurationen, informelle Administrationswege oder nicht nachvollziehbare technische Abhängigkeiten sind unzulässig.

Die Bereitstellung, der Betrieb sowie Leistungen zur z.B. Aufrechterhaltung und Wiederherstellung der Betriebsbereitschaft des Dienstes erfolgen auf der Grundlage eines EVB-IT Cloudvertrags (siehe **Anlage A0X**),

der durch einen Kriterienkatalog für Cloudleistungen ergänzt wird. Demzufolge sind ergänzend zu dieser Leistungsbeschreibung auch die Regelungen der EVB-IT Cloud-AGB zu beachten.

Das genaue Volumen der zu speichernden Daten kann aktuell nicht genau bestimmt werden. Die AG geht davon aus, dass zum Start dieser Leistung ein Volumen von 500 GB ausreichen sollte.

Die Nutzerzahl wird in der Testphase bei bis zu ca. 1.000 aktiven Nutzer*innen liegen. Es muss sichergestellt sein, dass diese Nutzer*innen den Service gleichzeitig nutzen können. Dabei ist zu berücksichtigen, dass die App nach Abschluss dieser Projektphase einem weitaus größeren Nutzerkreis zur Verfügung gestellt werden wird.
Das System muss daher bei Bedarf skalierbar sein, sodass sowohl der Speicherplatz wie auch die Nutzerzahl kurzfristig erhöht oder verringert werden können.
Das Konzept muss einen Lösungsvorschlag enthalten, wie diese Anpassungen umgesetzt werden können.

3. Anforderungen an das Cloud-Betriebsmodell

Der angebotene Cloud-Computing-Dienst muss über ein C5-Typ-2-Testat verfügen oder übergangsweise über eine Testierung oder Zertifizierung nach einem Standard gemäß der Verordnung über gleichwertige Sicherheitsnachweise zum C5-Standard für Cloud-Computing-Dienste im Gesundheitswesen (C5-Gleichwertigkeitsverordnung – C5GleichwV) vom 19. März 2025,

- Art der Cloud: Private Cloud, Private Government Cloud oder eine geeignete Alternative, wie z.B. Hybrid-Cloud, sofern sichergestellt werden kann, dass ausschließlich nicht-sensible Daten und/oder Dienste in der Public Cloud verarbeitet werden,
    - Managed Cloud Services: der AG steht mindestens eine Zugangsverwaltung zur Verfügung,
    - Nutzer: Die Infrastruktur muss ausreichend groß dimensioniert sein, um insbesondere im Rahmen der Validierungsstudien den Zugriff von ca. registrierten 1.000 Nutzer*innen (innerhalb definierter Zeiträume) zu gewährleisten.
    - Nutzerkreis: Hinsichtlich des Nutzerkreises soll keine Beschränkung bestehen.
    - Das System ist skalierbar, mindestens der Nutzungsumfang und die Speichergröße sind ohne größeren Aufwand anpassbar.
    - Endgeräte/Zugang: der Zugang wird größtenteils webbasiert über mobile Endgeräte (ios/Android) erfolgen und soll dementsprechend für diese Endgeräte optimiert sein.
    - Speicher: zur Speicherung der Daten der Auftraggeberin stellt der Auftragnehmer Speicherplatz in Höhe von zunächst 50GB bereit, der in der Vergütungspauschale für das Hosting inbegriffen ist.
    - Zur vertragsgemäßen Nutzung der vorgenannten Leistungen räumt der AN der AG die Nutzungsrechte gemäß den EVB-IT Cloud-AG Ziffer 14 ein. Abweichend davon gelten für die initialen Leistungen die Nutzungsrechte der EVB-IT Erstellungs-AGB und der in der Anlage A08 Leistungsverzeichnis dargestellten abweichenden und/oder ergänzenden Rechte.

Der Auftragnehmer hat die eingesetzte Cloudumgebung und alle eingesetzten KI-bezogenen Dienste der angebotenen Lösung vollständig und nachvollziehbar im Bieterkonzept 3 (siehe Anlage A10 Bieterkonzept) zu beschreiben.

4. Rechenzentrumsstandorte und Orte der Datenverarbeitung

Zu beachten sind bei der Wahl der Rechenzentrumsstandorte und den Orten der Datenverarbeitung die Vorgaben des Absatz 2 des §393 SGB V:

Die Verarbeitung von Sozial- und Gesundheitsdaten im Wege des Cloud-Computing-Dienstes darf nur

1.) im Inland,
2.) in einem Mitgliedstaat der Europäischen Union oder
3.) in einem diesem nach § 35 Absatz 7 des Ersten Buches gleichgestellten Staat oder, sofern ein Angemessenheitsbeschluss gemäß Artikel 45 der Verordnung (EU) 2016/679 vorliegt, in einem Drittstaat

erfolgen und sofern die datenverarbeitende Stelle über eine Niederlassung im Inland verfügt.

5. Anforderungen an KI-Modelle und KI-Dienste

Die angebotene KI-basierte Lösung muss mit den Anforderungen des EU AI Act sowie mit den einschlägigen europäischen und nationalen Datenschutz- und Sicherheitsanforderungen vereinbar sein.

Der Bieter hat im Bieterkonzept 3 – Cloud-, Sicherheits- und Datenschutzkonzept (siehe Anlage A10 Konzeptabfrage) offenzulegen, welche KI-Modelle, Modellanbieter, Infrastrukturen und Unterauftragnehmer eingesetzt werden, in welchem Rechts- und Betriebsraum diese betrieben werden und ob Drittstaatenbezüge bestehen oder nicht ausgeschlossen werden können.

Soweit im Rahmen der angebotenen Lösung KI-Modelle, Foundation Models, externe Inferenzdienste oder sonstige algorithmische Dienste eingesetzt werden, gelten ergänzend folgende Anforderungen:

- Der Einsatz ist vollständig offenzulegen.
- Nicht offengelegte Drittstaatenzugriffe auf Eingabe-, Ausgabe-, Protokoll- oder Metadaten sind unzulässig.
- Der Auftragnehmer hat die in der Software vorgesehenen KI-Komponenten fachlich, technisch und regulatorisch nachvollziehbar zu spezifizieren. Dabei ist insbesondere darzustellen, welche Funktionen regelbasiert, datenbankbasiert, KI-gestützt oder durch Large-Language-Model-/Retrieval-Augmented-Generation-Ansätze umgesetzt werden sollen. Zu berücksichtigen sind technische Dokumentation, Transparenz, Protokollierung, Genauigkeit, Robustheit und Cybersicherheit.

Zu beachten sind in diesem Kontext auch die folgenden Vorgaben:

- Trennung zwischen evidenzbasierter Wissensbasis, regelbasierten Entscheidungslogiken, KI-generierten Vorschlägen und ärztlich zu bestätigenden Handlungsempfehlungen.
- KI-Ausgaben dürfen keine autonome medizinische Entscheidung darstellen, sondern sind als entscheidungsunterstützende Vorschläge im Sinne eines Human-in-the-Loop-Ansatzes auszugestalten.
- Patientendaten dürfen nicht zum Training externer KI-Modelle verwendet werden.
- Anforderungen an Protokollierung, Audit-Trails und Reproduzierbarkeit: Es muss nachvollziehbar sein, auf welcher Datengrundlage, Wissensbasis, Modellversion und Logik eine Empfehlung erzeugt wurde.

6. Datenverarbeitung und Datenkategorien

Der Auftragnehmer hat darzustellen, welche Arten von Daten im Rahmen der Cloudleistungen verarbeitet werden. Hierzu gehören insbesondere personenbezogene Daten, sensible Gesundheitsdaten, Nutzungs- und Protokolldaten, Ein- und Ausgabedaten KI-basierter Komponenten, Konfigurations- und Systemdaten, Sicherungsdaten, Support- und Administrationsdaten sowie gegebenenfalls Test- und Evaluationsdaten.

Produktivdaten, Testdaten und sonstige Datenbestände sind technisch und organisatorisch voneinander zu trennen. Für Test-, Entwicklungs- und Evaluationsumgebungen sind nach Möglichkeit synthetische, anonymisierte oder anderweitig datenschutzkonforme Testdaten einzusetzen.

7. Unterauftragnehmer und Lieferkette

Der Einsatz von Unterauftragnehmern, Nachunternehmern, Modellanbietern oder sonstigen Drittanbietern ist nur zulässig, soweit diese gegenüber dem Auftraggeber vollständig offengelegt werden und die Anforderungen dieses Leistungsverzeichnisses erfüllen.

Für jeden eingesetzten Unterauftragnehmer sind vom Auftragnehmer nach Erhalt des Zuschlags mindestens die folgenden Daten anzugeben: Name des Unternehmens, Rolle im Leistungsgefüge, Art der erbrachten Leistung, Art des Zugriffs auf Daten oder Systeme, Ort der Leistungserbringung und betroffene Systembestandteile.

8. Drittstaatenbezüge

Der Auftragnehmer hat ausdrücklich darzustellen, ob im Rahmen der Cloudleistungen oder der eingesetzten KI-Dienste ein Drittstaatenbezug besteht oder nicht ausgeschlossen werden kann.

Als Drittstaatenbezug gelten insbesondere Speicherung oder Verarbeitung außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums, KI-Inferenz oder Modellbereitstellung außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums, Fernwartung oder Remote-Administration aus Drittstaaten, Zugriffsmöglichkeiten konzernverbundener Unternehmen aus Drittstaaten sowie Supportleistungen aus Drittstaaten.

9. Informationssicherheitsanforderungen

Die Cloudleistungen müssen so ausgestaltet sein, dass ein angemessenes Sicherheitsniveau für die verarbeiteten Daten und Systeme gewährleistet ist. Der Auftragnehmer hat insbesondere geeignete Maßnahmen zu Authentisierung, Autorisierung, Verschlüsselung, Protokollierung, Monitoring, Schwachstellenmanagement, Patchmanagement, API- und Schnittstellenabsicherung, Fernwartung, Backup und Wiederherstellung umzusetzen.

10. Datenschutz und technische und organisatorische Maßnahmen

Der Auftragnehmer hat die Cloudleistungen datenschutzkonform zu erbringen und geeignete technische und organisatorische Maßnahmen zum Schutz personenbezogener und sensibler Gesundheitsdaten umzusetzen.

Die wesentlichen TOM sind im Rahmen des Angebots lösungsbezogen darzustellen. Darüber hinaus ist der von der Auftraggeberin bereitgestellte Auftragsverarbeitungsvertrag vollständig auszufüllen; die dort geforderte TOM-Anlage ist konkret, vollständig und konsistent mit dem eingereichten Cloud-, Sicherheits- und Datenschutzkonzept auszufüllen.

11. Support-, Administrations- und Wartungszugriffe

Support-, Administrations- und Wartungszugriffe auf die Cloudumgebung dürfen nur in einem geregelten, dokumentierten und abgesicherten Verfahren erfolgen. Privilegierte Zugriffe sind nach dem Need-to-know- und Need-to-do-Prinzip zu vergeben, zu protokollieren und zeitlich sowie inhaltlich zu begrenzen.

12. Backup, Wiederherstellung und Notfallvorsorge

Der Auftragnehmer hat ein dokumentiertes Backup-, Wiederherstellungs- und Notfallkonzept vorzuhalten. Dieses muss mindestens Regelungen zu Art und Frequenz von Datensicherungen, Speicherort, Schutz der Sicherungsdaten, Wiederherstellbarkeit, regelmäßiger Überprüfung der Wiederherstellungsverfahren, Notfallorganisation und Wiederanlauf enthalten.

Der Auftragnehmer ist zur Erstellung von Backups der Daten der Auftraggeberin verpflichtet. Gegenstand des Backups sind sämtliche Daten, die von der AG in der Anwendung gespeichert werden. Die Erstellung von Backups soll täglich erfolgen. Eine Löschung von Backups soll nach Möglichkeit frühestens nach drei Monaten erfolgen. Dem Angebot ist ein Lösungsvorschlag beizufügen, wie die Datensicherung konkret umgesetzt werden könnte, ergänzend zur Nr. 16 der Anlage Kriterienkatalog für Cloudleistungen.

Sofern die AG die Unterstützung des AN zur Erstellung zusätzlicher BackUps oder zur Wiederherstellung von Daten anfordert, kann für diese Leistungen eine angemessene Vergütung vereinbart werden, auf Grundlage der im EVB-IT Cloudvertrag vereinbarten Vergütungssätze zur Vergütung von Leistungen von Personen nach Aufwand.

Leistungen, die bereits in der monatlich zu zahlenden Pauschale für die Bereitstellung und Nutzung des Clouddienstes enthalten sind oder im Rahmen der vertraglich vereinbarten Störungsbeseitigung, Mängelbeseitigung o.ä. auf Kosten des AN oder eines Unterauftragnehmers zu beseitigen sind, sind von dieser Regelung ausgenommen.

13. Datenexport/ Datenimport

Für den Export und Import von Daten stellt der Auftragnehmer der Auftraggeberin eine Möglichkeit zur Verfügung.
Der AN leistet im Bedarfsfall, auf Anforderung, Unterstützung beim Export und Import von Daten der Auftraggeberin.

14. Betriebs- und Supportleistungen

Als Teilleistung erbringt der AN Betriebs- und Supportleistungen. Diese sind in einer Weise zu erbringen, die einen stabilen, sicheren und nachvollziehbaren Betrieb der Lösung sicherstellt. Serviceparameter, Reaktionszeiten und Eskalationsstufen sind im Vertrag konkret festzulegen.

14.1 Betriebsleistungen

In den Themenbereich Betriebsleistungen fallen nach Ansicht der Auftraggeberin die folgenden Teilleistungen:

- Technischer Betrieb bzw. Unterstützung des Betriebs, Monitoring der IT-Infrastruktur, Anwendungen und Services, Patch- und Update-Management.
- Bereitstellung, Konfiguration und Pflege der vereinbarten Produktiv- und produktionsnahen Umgebungen.
- Durchführung von Deployments, Releasewechseln und Rollbacks nach abgestimmtem Verfahren.
- Technisches Monitoring, Überwachung zentraler Dienste sowie Alerting bei Störungen oder Kapazitätsproblemen.
- Mitwirkung an Wiederanlauf- und Notfallverfahren.

14.2 Supportleistungen

In den Themenbereich Supportleistungen fallen nach Ansicht der Auftraggeberin die folgenden Teilleistungen:

- Bereitstellung eines technischen Supports für die Auftraggeberin und – soweit vereinbart – für definierte Nutzergruppen.
- Bearbeitung von Anfragen zu Bedienung, Konfiguration, Fehlerbildern, Zugängen und technischen Auffälligkeiten.
- Nachvollziehbare Kommunikation von Bearbeitungsstand, Lösungsschritten und ggf. Workarounds.

Service Levels

- Für Support- und Betriebsleistungen sind Servicezeiten, Reaktionszeiten, Wiederherstellungsziele und Priorisierungsklassen festzulegen.
- Die Auftragnehmerin bzw. der Auftragnehmer hat geeignete Nachweise über die Einhaltung vereinbarter Service Levels zu führen.

Servicezeiten

Der Servicezeitraum ist Montag bis Freitag 8:00 Uhr bis 18:00 Uhr.

15. Incident-Management und Meldepflichten

Der Auftragnehmer hat ein geregeltes Verfahren zum Umgang mit Sicherheitsvorfällen, Datenschutzvorfällen und erheblichen Betriebsstörungen vorzuhalten. Das Verfahren muss Erkennung und Klassifikation von Vorfällen, interne Eskalationswege, unverzügliche Information des Auftraggebers bei relevanten Vorfällen, Maßnahmen zur Schadensbegrenzung sowie Dokumentation und Ursachenanalyse umfassen.

Zur Beseitigung von Störungen hat der Auftragnehmer alle für die Störungsbeseitigung zur Wiederherstellung der Betriebsbereitschaft* notwendigen Maßnahmen gemäß Ziffer 11 der EVB-IT Cloud-AGB zu ergreifen.

15.1 Meldung von Störungen

Der AN stellt ein Verfahren zur Meldung von Störungen zur Verfügung. Störungen müssen von der DSHS 24 Stunden an allen Tagen, inklusive Feiertage gemeldet werden können. Die Störungsmeldungen sowie die Antworten des Auftragsnehmers müssen auf Deutsch oder auf Englisch erfolgen.

Folgende Arten der Störungsmeldung werden 24/7 durch den Auftragnehmer angeboten:

- E-Mail oder Web Service Portal (Abgesichertes Service Portal mit Kundenauthentifizierung)

15.2 Störungsbeseitigung, Incident- und Problem-Management

Die nachfolgend beschriebenen Maßnahmen zur Beseitigung von Störungen sind während der Vertragslaufzeit vom Auftragnehmer zu leisten, sie gelten während des laufenden Projektzeitraumes als Mindestanforderung.

Maßnahmen zur Wiederherstellung der Betriebsbereitschaft (Incident Management)

- Annahme, Klassifikation, Bearbeitung und Nachverfolgung technischer Störungen und Fehlermeldungen.
- Unterscheidung zwischen Incident, Problem, Service Request und Change Request.
- Eskalation kritischer Störungen nach definierten Eskalationswegen.

- Strukturierte Erfassung, Priorisierung und Bearbeitung von Fehlern, die im Rahmen der Qualitätssicherung und Testung erkannt werden, einschließlich Nachtestung und Nachweis der Fehlerbehebung.
- Dokumentation der Bearbeitungsschritte, Statusmeldungen und Ursachenanalysen.

Reaktionszeiten im Incident Management

Im Rahmen dieses Verfahrens werden die folgenden Reaktionszeiten definiert und vertraglich vereinbart. Diese werden über eine separate, monatlich abzurechnende Servicepauschale für Pflegeleistungen vergütet.

Leistungen	**Mindestanforderungen**
1) Zeitraum für Eingang von Störungsmeldungen	365 x 7 x 24 Stunden
2) Reaktionszeit bei einer schwerwiegenden Störung	Bis spätestens um 12:00 Uhr am darauffolgenden Werktag
3) Reaktionszeit bei einer erheblichen Störung	Bis spätestens um 12:00 Uhr am zweiten darauffolgenden Werktag
4) Reaktionszeit bei einer leichten Störung	Innerhalb von 7 Kalendertagen
5) Wiederherstellungszeit	24 Stunden

- Zu 1.) Definition des Incident Management Prozess: Störungen können von der DSHS 24 Stunden/Tag an den Support des Auftragnehmers gerichtet werden. Mit Eingang der Störung beim Auftragnehmer wird mit der Bearbeitung im Rahmen der definierten Reaktionszeit begonnen.
- Zu 2.bis 4.) Definition siehe EVB-IT Cloud-AGB Ziffer 10 Störungsklassifizierung.
- Zu 5.) Störungen werden innerhalb der Wiederherstellungszeit im Rahmen der technischen Machbarkeit behoben. Die Wiederherstellungszeit wird definiert als der Zeitraum zwischen Eingang der Störungsmeldung und Wiederherstellung der Grundfunktionen des Systems. Die Wiederherstellung kann auch durch einen Workaround erfolgen, welcher durch eine später durchgeführte endgültige Störungsbeseitigung aufgehoben wird. Die Wiederherstellungszeit beträgt **24 Stunden, sofern keine abweichenden Vereinbarungen getroffen wurden**.
  Nach der erfolgreichen Behebung der Störung wird die Auftraggeberin umgehend über die Wiederherstellung der Betriebsbereitschaft informiert.

16. Verfügbarkeit, Wartungsfenster und Betriebsstabilität

Die Cloudumgebung ist so bereitzustellen, dass ein stabiler und nachvollziehbarer Betrieb der angebotenen Lösung gewährleistet ist. Der Auftragnehmer hat mindestens angestrebte Verfügbarkeiten, Wartungsfenster, Monitoring der Betriebsstabilität sowie Verfahren zur Störungsbehebung und Wiederaufnahme des Betriebs darzustellen.

16.1 zu erfüllende Anforderungen

- Die Mindestanforderungen während der Projektlaufzeit an die Verfügbarkeit entsprechen den in den EVB-IT Cloud Ziffer 8 dargestellten Anforderungen.

- Perspektivisch muss eine Ausweitung auf 0:00 bis 24:00 Uhr möglich sein.

17. Exit-Fähigkeit, Datenportabilität und Löschung

Der Auftragnehmer hat die Cloudleistungen so auszugestalten, dass bei Vertragsende, Anbieterwechsel oder sonstiger Beendigung des Betriebs eine geordnete, sichere und vollständige Übergabe möglich ist. Dies umfasst insbesondere vollständige Rückgabe relevanter Daten in einem gängigen, strukturierten und

weiterverarbeitbaren Format, Rückgabe oder Dokumentation relevanter Konfigurationsstände sowie sichere und nachweisbare Löschung verbliebener Datenbestände.

Die Bereitstellung der Daten der AG muss gemäß den EVB-IT Cloud AGB Ziffer 13.1 in Verbindung mit Ziffer 7.3 erfolgen. Die Bereitstellung umfasst alle für einen ordnungsgemäßen Exit erforderlichen Dokumentationen, Konfigurationsstände, Exportmöglichkeiten und Übergabeartefakte.

Im Rahmen einer Migration leistet der Auftragnehmer Unterstützung gemäß Ziffer 13.2 der EVB-IT Cloud-AGB, um einen geordneten Übergang des Betriebs oder der Weiterentwicklung auf die Auftraggeberin oder einen Dritten.

18. Reporting und Steuerung

• Regelmäßige Berichte über Betriebszustand, Störungen, Sicherheitsereignisse, offene Probleme, Releases und wesentliche Maßnahmen.

• Bereitstellung einer Übersicht wiederkehrender Fehlerbilder und identifizierter Verbesserungsbedarfe.

19. Schnittstellen- und Interoperabilitätsanforderungen

Die angebotene Lösung ist so zu konzipieren und umzusetzen, dass eine strukturierte und sichere Anbindung an relevante Systeme des deutschen Gesundheitswesens technisch vorbereitet oder - soweit beauftragt - umgesetzt werden kann.

Dies betrifft insbesondere Anbindungen an Praxisverwaltungssysteme (PVS), an Komponenten und Anwendungen der Telematikinfrastruktur, an die elektronische Patientenakte (ePA) sowie an sonstige interoperable Daten- und Kommunikationsdienste im Versorgungskontext.

- Anbindungen an Praxisverwaltungssysteme (PVS) bzw. Primärsysteme
- Anbindungen an Komponenten und Anwendungen der Telematikinfrastruktur
- Anbindungen an die elektronische Patientenakte (ePA)
- Anbindungen an interoperable Kommunikations- und Austauschdienste
- Import- und Export standardisierter Datenformate
- dokumentierte und versionierte Schnittstellen mit definierten Test- und Freigabeprozessen

20. Anforderungen an PVS-nahe Integration

Der Auftragnehmer hat darzustellen, wie eine Anbindung an Praxisverwaltungssysteme technisch vorgesehen ist. Schnittstellen sind so zu gestalten, dass sie eine praxistaugliche Integration mit minimalem Medienbruch, klarer Nutzerführung und nachvollziehbarem Datenfluss unterstützen.

Die Lösung soll so gestaltet sein, dass patienten- und fallbezogene Informationen, Dokumente, strukturierte Daten sowie Rückmeldungen aus EviGAIN medienbrucharm in bestehende Primärsysteme integriert oder aus diesen übernommen werden können, soweit dies fachlich erforderlich und technisch zulässig ist.

21. Anforderungen an ePA- und TI-Anschlussfähigkeit

Soweit die angebotene Lösung auf Daten der ePA zugreifen, ePA-relevante Inhalte verarbeiten oder perspektivisch in TI-nahe Versorgungsszenarien eingebunden werden soll, ist die Lösung so auszugestalten,

dass sie mit den jeweils geltenden Spezifikationen, Sicherheitsanforderungen und Rollenmodellen der gematik kompatibel weiterentwickelt werden kann.

Für Schnittstellen zur ePA bzw. zu Primärsystemen sind die von der gematik vorgesehenen Implementierungsleitfäden, Sicherheitsvorgaben und interoperablen Austauschformate zu berücksichtigen. Soweit Dokumente oder strukturierte Inhalte in die ePA eingestellt, daraus gelesen oder darüber referenziert werden, ist eine Anschlussfähigkeit an die jeweils geltenden ePA-Formate und Fachmodule sicherzustellen.

- Berücksichtigung geltender gematik-Spezifikationen und Implementierungsleitfäden für Primärsysteme,
- Berücksichtigung der Anforderungen an Sicherheitsarchitektur, Rollen und Berechtigungen der Telematikinfrastruktur,
- Berücksichtigung ePA-bezogener strukturierter Formate und Austauschmechanismen,
- Vorbereitung für dokumentenbasierte und strukturierte Interaktionen mit der ePA,
- Unterstützung eines nachvollziehbaren, revisionssicheren Datenflusses zwischen Primärsystem, EviGAIN und ePA.

22. Interoperabilitätsstandards

Die angebotene Lösung muss einen standardorientierten Interoperabilitätsansatz unterstützen. Soweit fachlich einschlägig, sind offene und im Gesundheitswesen etablierte Standards zu berücksichtigen, insbesondere HL7 FHIR, IHE-basierte Integrationsmuster, standardisierte Dokumenten- und Kommunikationsformate sowie fachliche Profile und Leitfäden der zuständigen Stellen.

Bei strukturierten Datenobjekten ist ein API-first-Ansatz vorzusehen. Schnittstellen sind so zu dokumentieren, zu versionieren und zu testen, dass ein sicherer, nachvollziehbarer und wartbarer Datenaustausch möglich ist.

- HL7 FHIR für strukturierte Gesundheitsdaten, soweit fachlich einschlägig
- IHE-orientierte Integrationsmuster und gematik-nahe Austauschmechanismen, soweit relevant
- standardisierte Dokumenten- und Kommunikationsformate
- versionierte API-Dokumentation und nachvollziehbare Fehlerbehandlung
- Trennung zwischen fachlicher Semantik, technischer Schnittstelle und Implementierungslogik

23. Kommunikations- und Austauschdienste

Soweit im Projektkontext relevant, ist die Lösung so auszulegen, dass eine spätere Anbindung an etablierte Kommunikationsdienste des Gesundheitswesens, etwa KIM-basierte Übermittlungswege oder andere standardisierte Austauschverfahren, technisch vorbereitet werden kann.

Der Auftragnehmer hat darzustellen, wie Dokumenten- und Datenaustausch, Signaturanforderungen, Berechtigungslogik und Rückmeldemechanismen in einer interoperablen Zielarchitektur berücksichtigt werden.

24. Nachweise und einzureichende Unterlagen

Der Auftragnehmer hat im Rahmen des Angebots alle für die Bewertung der Cloud-, KI- und Schnittstellenleistungen erforderlichen Unterlagen einzureichen.

Hierzu gehören mindestens eine lösungsbezogene Beschreibung der Cloudumgebung, Angaben zu Cloud-Anbietern, Modellanbietern, Standorten und Datenflüssen, Angaben zu eingesetzten KI-Modellen und KI-Diensten, Angaben zu Unterauftragnehmern, Angaben zu etwaigen Drittstaatenbezügen, die Darstellung der

wesentlichen technischen und organisatorischen Maßnahmen, die Darstellung der EU AI-Act-bezogenen Compliance- und Governance-Maßnahmen sowie der ausgefüllte Auftragsverarbeitungsvertrag einschließlich TOM-Anlage.

25. Mindestanforderungscharakter

Die in diesem Kapitel beschriebenen Anforderungen an Cloud-, KI- und Schnittstellenleistungen sind verbindliche Mindestanforderungen.

Angebote, die diese Anforderungen nicht erfüllen, nur unvollständig adressieren oder keine belastbare und nachvollziehbare Umsetzung erkennen lassen, können von der weiteren Wertung ausgeschlossen werden, soweit dies nach den Vergabeunterlagen vorgesehen ist.

Übersicht der besonders hervorzuhebenden Mindestanforderungen

Themenfeld	Mindestanforderung	Besonderer Fokus in der Angebotsprüfung
Cloud	Vollständige Offenlegung von Modell, Anbieter, Standorten, Unterauftragnehmern und Drittstaatenbezügen	Transparenz und Konsistenz der Betriebsarchitektur
Datenschutz/TOM	Lösungsbezogene TOM und vollständiger AVV	Schutz sensibler Gesundheitsdaten
KI	EU AI-Act-kompatible Governance, Human Oversight, Nachvollziehbarkeit	Modelltransparenz und europäische Souveränität
Schnittstellen	Vorbereitung bzw. Umsetzung standardorientierter Schnittstellen	Anschlussfähigkeit an PVS, ePA und TI
Exit	Datenportabilität, dokumentierte Übergabe, nachweisbare Löschung	Vermeidung von Vendor Lock-in