

Lfd. Nr.	Dokument (*)	Seite	Kapitel	Textstelle	Frage	Antwort
37	03_P1000_Leistungsbeschreibung	30	6.2.1.3 Eignungskriterien Nr.6	Geben Sie einen kurzen Überblick über das technische Equipment, welches Ihnen zur Verfügung steht und von Ihnen zur Erbringung der hier ausgeschriebenen Leistung, insbesondere bei der Durchführung der Erprobung in AP 5 eingesetzt wird. Mindestanforderung: Der Bieter ist aus Sicht des BSI in der Lage, die hier zu vergebende Leistung mit Hilfe der beschriebenen technischen Ausrüstung erfolgreich zu erbringen.	Wir bitten um Klarstellung, was im Rahmen dieses Projekts konkret als „technisches Equipment“ im Sinne des Eignungskriteriums zu verstehen ist. Nach unserer Auffassung wird die Durchführung von Tests und Evaluationen am realen Use Case voraussichtlich vor Ort auf den Systemen des jeweiligen Use Case Partners stattfinden. Gibt es seitens des BSI hierzu eine abweichende Erwartung? Sollte mit dem „technischen Equipment“ die Bereitstellung von zusätzlicher Rechenkapazität durch den Auftragnehmer gemeint sein, bitten wir um Information, wie in diesem Fall die Abrechnung der damit verbundenen Kosten erfolgen soll. Darüber hinaus bitten wir um Auskunft, ob unter „technische Ausrüstung“ ggf. auch Software, Prüftools und Werkzeuge zu verstehen sind. Falls dies zutrifft, kann seitens des BSI bestätigt werden, dass das Einbringen solcher Software-Ressourcen im Rahmen dieses Eignungskriteriums keine	Die tatsächliche Prüfung des Use-Cases muss nicht notwendigerweise beim Use-Case Partner auf dessen Hardware durchgeführt werden, diese kann je nach Möglichkeit auch beim Auftragnehmer durchgeführt werden. Ferner wird für den Aufbau, ggf. notwendige Anpassungen und den Test/Einarbeitung in die entsprechenden Werkzeuge eine entsprechende Hardware beim Auftragnehmer benötigt, die dieser für die Aufgaben nutzen kann. Eine Bereitstellung von Rechenkapazität für den Auftraggeber oder eine gesonderte Vergütung für entstehende Rechenkosten des Auftragnehmers sind nicht vorgesehen (vgl. hierzu auch Frage 1). Bezüglich der Nutzungsrechte verweise ich auf Frage 17: An bereits vor Projektbeginn bestehender Software, Methoden, Mustern, Hilfsmitteln, Modellen, Systemen und Tools benötigen wir nur insoweit Nutzungsrechte, wie diese für die Nutzung der Teil- und Gesamtleistung erforderlich sind. Die in diesem Vertrag vereinbarte Vergütung umfasst die Kosten der Einräumung und Übertragung der vorgenannten Rechte.

Lfd. Nr.	Dokument (*)	Seite	Kapitel	Textstelle	Frage	Antwort
					Übertragung von Nutzungsrechten an das BSI nach sich zieht? Für eine entsprechende Klarstellung danken wir Ihnen.	
38	03_P1000_Leistungsbeschreibung	16	3.2	Die Projektlaufzeit beginnt mit dem Datum der Auftragserteilung (Projektstart) und endet 6 Kalenderwochen nach der durch den Auftragnehmer im Angebot festgelegten Dauer für die Auftragsdurchführung. Für die Fertigstellung des Projektes wird vom AG dabei ein Zeitrahmen von maximal 18 Kalendermonaten verbindlich vorgegeben.	Wir bitten um Klarstellung, welchen Zeitraum das BSI als bevorzugten Starttermin für das Projekt vorsieht. Nach Kapitel 3.2 der Leistungsbeschreibung beginnt die Projektlaufzeit mit dem Datum der Auftragserteilung; ein expliziter bevorzugter Starttermin wird jedoch nicht genannt. Gibt es seitens des BSI Vorgaben oder Präferenzen hinsichtlich des Projektbeginns, die bei der Angebotsplanung zu berücksichtigen sind? Für eine entsprechende Information danken wir Ihnen.	Nach aktueller Planung ist ein Projektstart Ende September am wahrscheinlichsten, dies ist aber nicht genau vorgegeben.
39	03_P1000_Leistungsbeschreibung	9	Kapitel 2.3	Die durch den AN aufzustellenden Prüfkriterien, Prüfanforderungen und Best Practices haben das Ziel, die Abdeckung aller sicherheitsbezogenen Risiken, die den vertrauenswürdigen Einsatz von agentischen KI-Systemen berühren, zu erreichen. In diesem Sinne sind sowohl die Schutzziele der klassischen IT-Sicherheit, als auch die im Kontext der KI-Sicherheit relevanten Dimensionen der Datenqualität und -verwaltung, Funktionalität, Sicherheit, Transparenz und Erklärbarkeit bei der Ausgestaltung der	Im Zusammenhang mit den qualitativen Zuschlagskriterien 1.1 und 1.2 (Kapitel 6.2.1.4) bitten wir um eine Klarstellung hinsichtlich des inhaltlichen Fokus der geforderten Ausarbeitungen. In der Beschreibung von Arbeitspaket 3 (Kapitel 2.3) werden mögliche Prüfdimensionen genannt, die explizit über einen engen Cybersicherheitsbegriff hinausgehen und klassische Dimensionen von KI-Vertrauenswürdigkeit wie Transparenz, Fairness oder menschliche Aufsicht einschließen. In den Anweisungen zu	Für die Ausarbeitungen zu 1.1 und 1.2 können die KI- und IT-spezifischen Sicherheitsdimensionen, insbesondere auch die der agentischen KI herangezogen werden. Wie weitgehend der Katalog im Projekt über die Kernthemen der IT- und KI-Sicherheit hinausgeht, wird während des Projektes genau festgelegt, muss aber kein Teil der hier geforderten Ausarbeitungen sein.

Lfd. Nr.	Dokument (*)	Seite	Kapitel	Textstelle	Frage	Antwort
				Prüfkriterien und Prüfanforderungen zu betrachten. Die nachfolgend aufgezählten Dimensionen können bei der Formulierung der Prüfkriterien und -anforderungen herangezogen werden: [...] Menschliche Aufsicht (Human Oversight), Fairness, Transparenz, Datenqualität & -management, Entwicklung [...]	1.1 und 1.2 wird hingegen ausschließlich auf Bedrohungen und Risiken aus dem Bereich der KI-spezifischen Cybersicherheit fokussiert. Wie ist dieser Unterschied zu interpretieren? Ist es korrekt, dass der zu erarbeitende Prüfkatalog einen erweiterten Sicherheitsbegriff im Sinne der Vertrauenswürdigkeitsdimensionen zugrunde legen soll, oder sollen sich die Ausarbeitungen zu 1.1 und 1.2 explizit nur auf die Dimension der KI-spezifischen Sicherheit beziehen? Für eine entsprechende Klarstellung danken wir Ihnen.	

(*) Leistungsbeschreibung, Projektvertrag, Bekanntmachung, allgemeine Frage, etc.