Bieterfragen

Frage 1: Nach Kapitel 2 der Zuschlagsmatrix sind die zwingenden Anforderungen der Leistungsbeschreibung Mindestanforderungen; nach Kapitel 26 Nr. 18 der Leistungsbeschreibung sind erkennbare Abweichungen oder Einschränkungen darzustellen. Bitte teilen Sie mit, welche Anforderungen als "zwingend" zu verstehen sind - nur die mit „muss“ formulierten oder auch die mit „soll“ bzw. „mindestens“ formulierten? Gehören insbesondere die in Kapitel 18 und 19 genannten Werte (u. a. Verfügbarkeit, Reaktions- und Wiederherstellungszeiten, RTO, Wartungstermine) dazu? Führt eine nach Kapitel 26 Nr. 18 dargestellte Abweichung von einer Mindestanforderung zwingend zum Ausschluss? Bitte erläutern Sie, wie Kapitel 26 Nr. 18 zu verstehen ist.

Antwort zu Frage 1:

Die mit „muss“ formulierten Anforderungen sind als zwingend anzusehen. Für die mit „soll“ bzw. „mindestens“ formulierten Anforderungen muss selbstverständlich auch dargelegt werden, inwieweit diese erfüllt oder eben auch (zumindest teilweise) nicht erfüllt werden können. Dies gilt insbesondere auch für die Anforderungen aus Kapitel 18 und Kapitel 19. Diese unterliegen derselben Systematik, die für die gesamte Leistungsbeschreibung gilt.

Frage 2: Die Reaktions- und Behebungszeiten nach Kapitel 18.4 der Leistungsbeschreibung gelten innerhalb der Helpdeskzeiten, der Bemessungszeitraum nach Kapitel 19.1.1 umfasst dagegen 6–20 Uhr. Bitte erläutern Sie, ob die maximale ungeplante Ausfallzeit von einer Stunde am Stück auch für Störungen außerhalb der Helpdeskzeiten, aber innerhalb des Bemessungszeitraums gelten.

Antwort zu Frage 2:

Ja, die maximale ungeplante Ausfallzeit gelten innerhalb des Bemessungszeitraums, der über die reinen Helpdeskzeiten hinausgehen.

Frage 3: Bitte erläutern Sie, ob Softwareaktualisierungen, die ohne Unterbrechung der Verfügbarkeit eingespielt werden, als Wartungstermin im Sinne von Kapitel 19.1.4 der Leistungsbeschreibung gelten. Gilt die Begrenzung auf vier reguläre Wartungstermine je Kalenderjahr auch für Wartungsarbeiten, die vollständig außerhalb des Bemessungszeitraums stattfinden?

Antwort zu Frage 3:

Wenn Softwareaktualisierungen ohne Unterbrechung der Verfügbarkeit eingespielt werden, so gelten diese nicht als Wartungstermin im Sinne von Kapitel 19.1.4.

Ja, grundsätzlich dürfen nicht mehr als vier reguläre Wartungstermine je Kalenderjahr (auch außerhalb des Bemessungszeitraums) durchgeführt werden – Hintergrund ist die Ressourcenbindung auf Seiten des Auftraggebers.

Frage 4: Bitte teilen Sie mit, ob die RTO von vier Stunden nach Kapitel 19.2.2 der Leistungsbeschreibung auch für Großschadens- und Katastrophenszenarien nach Kapitel 19.4.6 (z. B. Ausfall eines gesamten Rechenzentrumsstandorts) gilt, oder sind hierfür gesonderte Werte vorgesehen bzw. anzubieten?

Antwort zu Frage 4:

Für Großschadens- und Katastrophenszenarien sind gesonderte Werte anzubieten.

Frage 5: Gehen wir recht in der Annahme., dass es sich bei den Werten in der Spalte „Ziel für Behebung beziehungsweise Wiederherstellung“ in Kapitel 18.4 der Leistungsbeschreibung um Zielwerte handelt?

Antwort zu Frage 5:

Hierbei handelt es um Anforderungen, die von Seiten des Auftraggebers an den neuen Auftragnehmer gestellt werden. Wir gehen davon aus, dass Sie uns diese Zielwerte zusichern können, ansonsten bedarf es hier eine eindeutige Kennzeichnung, welche abweichenden Werte hier veranschlagt bzw. zugesichert und angeboten werden.

Frage 6: Kapitel 19.2 der Leistungsbeschreibung legt nur RTO-Werte fest. Bitte teilen Sie mit, ob ein maximal zulässiger Datenverlust (RPO) erwartet wird, und ist dieser vom Bieter anzubieten?

Antwort zu Frage 6:

In der Leistungsbeschreibung ist RPO explizit nicht abgefragt. Dennoch wäre es wünschenswert, wenn Sie uns hier ein entsprechendes Angebot unterbreiten können (basierend auf Ihrem Leistungsspektrum oder vergleichbaren Referenzangeboten).

Frage 7: Gehen wir recht in der Annahme, dass die Anforderung „mindestens zwei technisch oder räumlich getrennte Speicherziele“ (Kapitel 19.3.2) als erfüllt anzusehen ist, wenn die Sicherungen getrennt von der Produktivumgebung in einem Rechenzentrum an einem anderen Standort vorgehalten werden?

Antwort zu Frage 7:

Ja, diese Annahme ist korrekt.

Frage 8: Gehen wir recht in der Annahme, dass der Übergang vom Rechenzentrum des Auftragnehmers in das öffentliche Netz bzw. dessen VPN-Endpunkt als Übergabepunkt zulässig ist? Falls nein: Teilen Sie bitte mit, welchen Übergabepunkt Sie im SaaS-Betrieb als Messpunkt nach Kapitel 19.1.3 der Leistungsbeschreibung ansehen.

Antwort zu Frage 8:

Folgende drei Anbindungsszenarien sind für uns denkbar:

- **Variante A: Die Mitarbeitenden greifen über das normale Internet (HTTPS) auf die SaaS-Software zu.**
- **Variante B: Zwischen dem Landratsamt bzw. IT-Verbund und PROSOZ wird eine feste VPN-Verbindung (Site-to-Site-VPN) aufgebaut.**
- **Variante C: Die Anbindung erfolgt über eine gesonderte Verbindung, beispielsweise über einen Netzbetreiber oder ein Behördennetz.**

Falls Sie noch weitere Anbindungsszenarien sehen, bitten wir Sie, diese aufzuführen und in diesem Kontext zu beschreiben.

Frage 9: Gehen wir recht in der Annahme, dass die Nutzung der Test- und Qualitätssicherungsumgebung für Schulungszwecke als „technisch gleichwertige Möglichkeit zur Durchführung von Schulungen“ im Sinne von

Kapitel 10.4 der Leistungsbeschreibung gilt?

Antwort zu Frage 9:

Sie sollten darlegen, inwiefern und inwieweit die Nutzung der Test- und Qualitätssicherungsumgebung für Schulungszwecke dafür geeignet ist oder worin ggf. auch die Grenzen oder auch Einschränkungen liegen (könnten).

Frage 10: Bitte teilen Sie mit, was Sie in Kapitel 9.1 unter „externen Zugriffen“ verstehen - Zugriffe von Nutzenden außerhalb seines Netzes oder Zugriffe Dritter, etwa des Supports? Ist die Anforderung für Nutzende erfüllt, wenn die Mehrfaktor-Authentifizierung über die Anmeldung per Microsoft Entra ID (Kapitel 6.5) durch den Auftraggeber durchgesetzt wird?

Antwort zu Frage 10:

Exakt, um Zugriffe solcher Art geht es hierbei unter anderem. Auch hierbei ist zwingend die Anmeldung per Microsoft EntralD zu realisieren.

Frage 11: Gehen wir recht in der Annahme, dass es für die Erfüllung des Kapitels 9.3 der Leistungsbeschreibung ausreichend ist, Zertifizierungen des Rechenzentrumsbetreibers (ISO/IEC 27001, BSI C5) zusammen mit eigenen Nachweisen des Bieters (technisch-organisatorische Maßnahmen, jährliche externe Penetrationstests) vorzulegen? Fließen die Nachweise in die Wertung ein?

Antwort zu Frage 11:

Bitte legen Sie alle Zertifizierungen und Nachweise vor, die auf diese Dokumentenkategorie einzahlen, auch wenn sie kein expliziter Bestandteil der Bewertungsmatrix sind.

Frage 12: Sie haben Ihren Vergabeunterlagen ein Dokument mit dem Namen "Technische Anforderungen Ausschreibungen - ITV.draft" beigefügt. Wir fragen höflich an, ob dieses Dokument versehentlich beigefügt wurde. Die Kennzeichnung "draft" ("Entwurf") lässt dies vermuten?

Hintergrund ist, dass sich hierin etliche Anforderungen finden, die für die Beschaffung einer Fachsoftware im Jugendamt deutlich zu hoch greifen dürften und eher aus dem Bereich der Beschaffung von Software z.B. im Verteidigungsbereich bekannt sind.
So fordern Sie etwa in Punkt 2.3 eine Hintergrundüberprüfung von Mitarbeitern vor der Einstellung. Diese Überprüfung ist im Bereich der Erstellung von Softwareprodukten im Jugendbereich völlig unüblich und lässt sich arbeitsrechtlich mangels rechtlicher Grundlage nicht umsetzen. Noch weniger kann dies in Bezug auf Subunternehmer beeinflusst werden.
Des Weiteren widersprechen sich die Anforderungen; so reicht es einerseits aus, die Basis-Sicherheitsmaßnahmen des BSI-Grundschutz-Katalogs zu erfüllen (Nr. 3.1), andererseits werden im gesamten Dokument deutlich weitergehende Maßnahmen gefordert.
Gehen wir daher recht in der Annahme, dass die Einhaltung der Basis-Sicherheitsmaßnahmen nach BSI-Grundschutzkatalog und die Einhaltung der Konformität nach ISO/IEC 27001 für diese Ausschreibung ausreichend sind?
Gehen wir ferner recht in der Annahme, dass die Anforderungen erfüllt sind, wenn der Rechenzetrumsbetreiber nach ISO/IEC 27001 zertifiziert und nach BSI C5 testiert ist und der Auftragnehmer ein eigenes ISMS betreibt?

Antwort auf Frage 12:

Dieses Dokument befindet sich noch im Aufbau und soll perspektivisch das Rahmenwerk für neue Systeme und Applikationen bilden.

Für diese Ausschreibung und demnach für Sie sind folgende drei Aspekte relevant:

- **Die Einhaltung der Basis-Sicherheitsmaßnahmen nach BSI-Grundschutz sind zwingend notwendig**
- **Die Einhaltung der Konformität nach ISO/IEC 27001 ist zwingend notwendig**
- **Eine Zertifizierung des Rechenzentrumsbetreibers nach ISO/IEC 27001 ist zwingend notwendig**

Alle weiteren in diesem Dokument aufgezeigten Punkte sind in diesem Kontext für Sie nicht gesondert zu beschreiben.