Geschäftszeichen: 3194.Z3-3_01-22-42

In dem Nachprüfungsverfahren

G… GmbH
vertreten durch …

Verfahrensbevollmächtigte…

- Antragstellerin -

gegen

Freistaat Bayern
vertreten durch…

Verfahrensbevollmächtigte: …

- Antragsgegner -

A… GmbH
vertreten durch …

Verfahrensbevollmächtigte: …

- Beigeladene -

Dienstgebäude
Maximilianstraße 39
80538 München
U4/U5 Lehel
Tram 16/19 Maxmonument

Telefon Vermittlung
+49 89 2176-0

Telefax
+49 89 2176-2914

E-Mail
poststelle@reg-ob.bayern.de

Internet
www.regierung.oberbayern.bayern.de

wegen der Vergabe Telenotarzt Systemlieferant erlässt die Regierung von Oberbayern – Vergabekammer Südbayern auf die mündliche Verhandlung vom 14.02.2023 durch die Vorsitzende, Frau Müller, die hauptamtliche Beisitzerin, Frau Orlick, und den ehrenamtlichen Beisitzer, Herrn Demharter, folgenden

Beschluss:

1. Dem Antragsgegner wird untersagt, den Zuschlag auf das Angebot der Beigeladenen auf Grundlage der bisherigen Wertung zu erteilen. Dem Antragsgegner wird bei fortbestehendem Beschaffungsabsicht aufgegeben, das Vergabeverfahren in den Stand vor der Prüfung der Angebote zurückzuversetzen und unter Berücksichtigung der Rechtsauffassung der Vergabekammer fortzuführen.

2. Der Antragsgegner und die Beigeladene tragen die Kosten des Verfahrens (Auslagen und Gebühren) gesamtschuldnerisch. Die zur zweckentsprechenden Rechtsverfolgung notwendigen Aufwendungen der Antragstellerin tragen Antragsgegner und Beigeladene zu gleichen Teilen.

3. Für das Verfahren wird eine Gebühr in Höhe von …,00 EUR festgesetzt. Auslagen sind nicht angefallen.

4. Die Hinzuziehung eines Verfahrensbevollmächtigten durch die Antragstellerin war notwendig.

Gründe:

I.

Mit Auftragsbekanntmachung vom 10.12.2021, veröffentlicht im Supplement zum Amtsblatt der Europäischen Union unter Nr. 2021/S 240-631589, schrieb der Antragsgegner einen Dienstleistungsauftrag über die Entwicklung, Herstellung, Lieferung, Montage, Installation und Inbetriebnahme eines TNA-Systems im Wege eines offenen Verfahrens aus. Zuschlagskriterien waren gemäß Abschnitt II.2.5) der Bekanntmachung der Preis mit einer Gewichtung von 30% sowie drei Qualitätskriterien.

Ausweislich der Angabe in Abschnitt I.3) der Bekanntmachung standen die Auftragsunterlagen für einen uneingeschränkten und vollständigen direkten Zugang gebührenfrei unter der dort genannten Internetadresse zur Verfügung.
Bestandteil der Vergabeunterlagen war unter anderem ein Muster eines Auftragsverarbeitungsvertrags nach Art. 28 Abs. 3 DSGVO (Datenschutz-Grundverordnung), welcher unter Ziffer 2 festlegte, dass der Ort der Leistungserbringung ausschließlich in der Bundesrepublik Deutschland, einem Mitgliedsstaat der Europäischen Union oder einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum liegen dürfe. Unter Ziffer 2.7.1 des Lastenhefts war festgelegt, dass der Auftragnehmer die Erfüllung der ihn betreffenden im Datenschutzkonzept dargestellten und regulatorischen datenschutzrechtlichen Anforderungen sicherstellen müsse. Unter Ziffer 4 des Lastenhefts wurde zudem aufgeführt, dass Ressourcen Standort und Datenverarbeitung des Cloud-Services für das TNA-System die Europäische Union bzw. der Europäische Wirtschaftsraum sein müssen. Unter Ziffer 1.3.1.6 der Wertungskriterien war für das Datenschutzkonzept als Ziel angegeben, dass auf Grundlage des Konzeptes gewährleistet sein soll, dass die Leistung des Bieters den Anforderungen der datenschutzrechtlichen Regulierungen entspricht und persönliche Daten höchstmöglich geschützt sind.

In einer Bieterfrage vom 22.02.2022 bat ein potentieller Bieter um Klarstellung, dass auch ein Cloud-Provider der seine Support-Leistungen aus der Schweiz erbringt zulässig sei, solange die IT-Infrastruktur des TNA-Systems in der EU stehe. Der Antragsgegner verneinte dies und erklärte die Eingrenzung auf die Europäische Union und den Europäischen Wirtschaftsraum bewusst getroffen zu haben, eine Ausweitung auf den Raum des Angemessenheitsbeschlusses werde nicht erfolgen.

Sowohl Antragstellerin als auch Beigeladene reichten fristgerecht ein Angebot ein. Das Angebot der Antragstellerin enthielt unter anderem in ihrem Betriebskonzept zum Cloud-Service die Aussage, dass die TNA-Cloud in den A… Datacenters in Deutschland (Frankfurt am Main & Berlin) betrieben werde und somit komplett in Deutschland gehostet werde.
Das Datenschutzkonzept der Antragstellerin enthielt unter anderem die Aussage, dass ruhende Daten sowie Datenübertragungen innerhalb und außerhalb der A…-Cloud grundsätzlich von M… verschlüsselt werden würden. Die genutzten Rechenzentren seien in Frankfurt am Main und in Berlin. Außerdem werde die Antragstellerin die Bring-Your-Own-Key-Funktionalität nutzen, hierfür werde der Zugangsschlüssel für die TNA-Cloud von der Antragstellerin selbst generiert und verwaltet. Weiter erklärte die Antragstellerin in ihrem Datenschutzkonzept, dass immer mindestens ein kundenseitiger Schlüssel verwendet werde um auf diese Weise sicherzustellen, dass M… oder Unterauftragnehmer zu keinem Zeitpunkt Zugriff auf die Daten in der TNA-Cloud erhalten können.

Im Rahmen der Angebotsprüfung richtete der Antragsgegner mit Schreiben vom 05.05.2022 ein Aufklärungsersuchen an die Antragstellerin. Darin erklärte er, dass die „in den Vergabeunterlagen niedergelegten (Leistungs-)Anforderungen […] so zu verstehen [sind], dass ein Angebot diesen Anforderungen dann nicht mehr entspricht, wenn nicht sichergestellt ist bzw. durch den/die Bieter/-in nicht sichergestellt werden kann, dass im Rahmen der Leistungserbringung personenbezogene Daten nicht den EWR verlassen. […] Ein Widerspruch mit den Anforderungen der Vergabeunterlagen bestehe insbesondere dann nicht, wenn ab dem Zeitpunkt der Erbringung des Cloud-Betriebs eine Übermittlung in potentielle Drittländer bereits technisch, organisatorisch und rechtlich ausgeschlossen ist. Ein Widerspruch mit den Anforderungen der Vergabeunterlagen und eine in Drittländern stattfindende Verarbeitung personenbezogener Daten läge zudem in einer zweiten Variante nicht vor, wenn alle Daten im Zugriffsbereich des Drittlandes so verarbeitet werden, dass eine Personenbeziehbarkeit ausgeschlossen ist bzw. werden kann. Die Konzeption des TNA-Systems habe eine Verarbeitung personenbezogener Daten auch in der Cloud zur Folge. Für die zweite Variante sei nach gegenwärtiger Fakten- und Rechtslage nach seiner Ansicht davon auszugehen, dass auch eine interne Verschlüsselung der Datenverarbeitung und Datenablage mit einem nutzereigenen Schlüssel keine hinreichende Gewähr für einen Schutz gegen etwaige Einsichtnahmen in die Daten bietet bzw. zu bieten vermag, da im Cloud-System selbst personenbezogene Daten verarbeitet werden. Dies setze technisch eine Entschlüsselung der Daten im Zugriffsbereich des Cloud-Betreibers voraus. Zudem werde der verwendete Nutzerschlüssel ebenfalls auf Komponenten in der Cloud-Infrastruktur abgelegt.“

Die Antragstellerin antwortete auf das Aufklärungsverlangen fristgerecht, dass sie die Vergabeunterlagen des Antragsgegners ebenfalls so verstanden habe, wie dieser nochmals im Schreiben vom 05.05.2022 ausgeführt habe und ihr Angebot diesen Vorgaben entspräche. Durch diverse technische, organisatorische und rechtliche Maßnahmen würde sichergestellt, dass zu keinem Zeitpunkt Daten in die USA oder in Drittländer übertragen würden und die Leistung ausschließlich im europäischen Wirtschaftsraum erbracht würde. Insbesondere stellte die Antragstellerin darin auch ausführlich dar, wie die Wartung und der Support durchgeführt würden.

Am 17.05.2022 schrieb der Antragsgegner an den Bayerischen Landesbeauftragten für den Datenschutz. In dem Schreiben fasste der Antragsgegner den Sachverhalt kurz auf einer Seite Text zusammen und teilte darin mit, dass die Antragstellerin die M… Cloud-Umgebung nutzen wolle, welche durch die M… Ltd. betrieben würde. Im Rahmen der Aufklärung sei seitens der Antragstellerin dargestellt worden, welche rechtlichen, technischen und organisatorischen Maßnahmen ergriffen würden, damit zu keinem Zeitpunkt personenbezogene Daten in die USA

oder andere Drittländer ausgeleitet oder übertragen würden. Durch entsprechende Verträge zwischen der Antragstellerin und M… könne eine Datenhaltung außerhalb der gewählten Regionen ausgeschlossen werden. Mithilfe der „A… Lockbox" wolle die Antragstellerin sicherstellen, dass Zugriff durch M…-Techniker nur nach vorheriger Zustimmung möglich sei. Um generell unerlaubte Zugriffe von Benutzern aus Drittländern zu verhindern, würde die Antragstellerin sämtliche Systeme in einem Alarm- und Monitoring—System überwachen. Die Antragstellerin würde nach Einschätzung des Antragsgegners alle durch M… technisch und vertraglich angebotenen Möglichkeiten bzgl. Datenverschlüsselung (gem. Angebot nutzerspezifischer Schlüssel, abgelegt in einem „A… Key Vault“) und geographischer Festlegungsmöglichkeit von Speicherorten (ERW/EU/DE) zur Nutzung für den Regelbetrieb des TNA—Systems vorsehen. Aus Sicht des Antragsgegners bleibe in der Aufklärung jedoch die kritische Fragestellung unbeantwortet, ob die Nutzung der technischen und vertraglichen Maßnahmen in der A…-Cloud ausreichend ist, um die Verarbeitung von personenbezogenen Daten in Drittländern (bei erzwungenem Datenzugriff) gänzlich ausschließen zu können. Daher bat der Antragsgegner den Bayerischen Landesbeauftragten für den Datenschutz unter anderem um eine Einschätzung, ob die von der Antragstellerin angebotene Leistung mit Blick auf die dargestellte Sachlage seiner Einschätzung nach datenschutzkonform sei.

Mit Schreiben vom 20.05.2022 antwortete der Bayerische Landesbeauftragte für den Datenschutz, dass er den Schutz durch die „A… Lockbox“ nicht für ausreichend halte, um Datenzugriffe durch M… im Rahmen von drittstaatlichen Auskunftsbegehren zu verhindern. Gelänge es nicht, effektive zusätzliche Maßnahmen zu implementieren, die gewährleisten, dass die in ein Drittland übermittelten personenbezogenen Daten ein der Sache nach gleichwertiges Schutzniveau genießen, dürfe in dem hier betrachteten Datenkontext nicht mit der Verarbeitung begonnen werden. Bei der geplanten Verarbeitung könne nach seinem Kenntnisstand derzeit nicht ausgeschlossen werden, dass personenbezogene Daten insbesondere US-Behörden durch M… offengelegt würden, ohne dass die neben den Standarddatenschutzklauseln hierfür erforderlichen zusätzlichen Schutzmaßnahmen wirksam umgesetzt würden.

Mit Schreiben vom 15.06.2022 und 13.07.2022 übersandte die Antragstellerin unaufgefordert weitere Informationen zu den rechtlichen und organisatorischen Maßnahmen sowie eine kurze Erläuterung der A… Lockbox Technologie.
Mit Schreiben vom 15.07.2022 übersandte sie eine Stellungnahme des Bayerischen Landesamts für Datenschutzaufsicht vom selben Tag, in der dieses mitteilte, dass die Beauftragung eines in der EU ansässigen Auftragsverarbeiters, der seine Datenverarbeitung ausschließlich innerhalb der EU und ohne Einschaltung von Subunternehmen in Drittstaaten durchführt, auch unter Berücksichtigung möglicher drittstaatlicher Datenzugriffsbegehren keine Datenübermittlung begründe, für die der Verantwortliche den besonderen Anforderungen der Art. 44 bis 47

und 49 der DSGVO unterliegt. Unabhängig davon bleibe jedoch bei Prüfung der Auftragsverarbeitungsvereinbarung genauer zu untersuchen, wie der Auftragsverarbeiter der Verpflichtung nach Art. 28 Abs. 3 Satz 2 Buchst. a) DSGVO nachzukommen vermag, Datenverarbeitungen nur im Rahmen dokumentierter Weisungen des Verantwortlichen oder zur Erfüllung solcher Pflichten zu verarbeiten, denen der Auftragsverarbeiter nach dem Recht der Europäischen Union oder der Mitgliedsstaaten unterliegt. Ebenso müsse im Rahmen der allgemeinen Zuverlässigkeitsbewertung nach Art. 28 Abs. 1 DSGVO genauer zu betrachten sein, welche Erkenntnisse hinsichtlich der Beachtung der Anforderungen des Art. 48 DSGVO vorliegen, der drittstaatliche Zugriffsbegehren u.a. gegenüber Auftragsverarbeitern unter den Vorbehalt stellt, dass die Übermittlung bzw. Offenlegung personenbezogener Daten auf eine wirksame internationale Übereinkunft wie etwa eines Rechtshilfeabkommens gestützt werden müsse.

Mit Informationsschreiben gemäß § 134 GWB vom 29.07.2022 setzte der Antragsgegner die Antragstellerin davon in Kenntnis, dass ihr Angebot ausgeschlossen werde, da der von der Antragstellerin angebotene Cloud-Betrieb nicht den Anforderungen der DSGVO entspräche. Das Angebot sei damit wegen unzulässiger Änderungen an den Vergabeunterlagen auszuschließen. Der Bayerische Landesbeauftrage für den Datenschutz sei mit Schreiben vom 20.05.2022 auf Grundlage aller relevanten Details, einschließlich der spezifischen Einzelheiten des Angebots der Antragstellerin, zu dem Ergebnis gekommen, dass in dem hier betrachteten Kontext mit der geplanten Verarbeitung von personenbezogenen Daten nicht begonnen werden dürfe. Für das von der Antragstellerin vorgesehene „Betriebskonzept Cloud-Service“ bestehe das Risiko, dass sich etwaige Auskunftsbegehren von Sicherheitsbehörden der USA, insbesondere auf Grundlage von Section 702 FISA bzw. des CLOUD Act, auf die in der Cloud vorhandenen Daten erstrecken. Die vorgesehenen technischen und organisatorischen Maßnahmen seien nicht geeignet, die Risiken solcher drittstaatlichen Auskunftsbegehren hinreichend zu kompensieren. Die verbleibenden Risiken könnten auch durch die benannten Verschlüsselungsmechanismen nicht kompensiert werden. Nach der Konzeption des TNA-Systems und darauf aufbauend dem Angebot finde eine Verarbeitung personenbezogener Daten unmittelbar in der Cloud statt, wobei allerdings die Schlüssel nicht alleine durch den Verantwortlichen oder den unmittelbar beauftragten Auftragsverarbeiter verwaltet und kontrolliert würden. Insofern würden „lesbare“ personenbezogene Daten im Zugriffsbereich des Cloud-Betreibers verarbeitet. Zudem teilte der Antragsgegner der Antragstellerin mit, dass beabsichtigt sei, den Zuschlag frühestens am 09.08.2022 auf das Angebot der Beigeladenen zu erteilen.

Mit Schreiben vom 03.08.2022 beanstandete die Antragstellerin die Vergabeentscheidung des Antragsgegners als vergaberechtswidrig. Die Prüfung und Wertung des Angebots der Antragstellerin sei fehlerhaft gewesen und benachteilige die Antragstellerin im Wettbewerb.

Mit Schreiben vom 05.08.2022 antwortete der Antragsgegner der Antragstellerin, dass ihren Rügen nicht abgeholfen werde. Die bestehenden technischen bzw. organisatorischen Maßnahmen würden nicht ausreichen um die aus drittstaatlichen Auskunftsersuchen erwachsenden Risiken hinreichend zu kompensieren. Damit bestehe eine Abweichung von den Anforderungen an die Leistungserbringung, der Antragsgegner müsse daher am Angebotsausschluss festhalten.

Nachdem den Rügen der Antragstellerin nicht abgeholfen wurde, stellte die Antragstellerin mit Schreiben vom 08.08.2022 einen Nachprüfungsantrag gem. § 160 Abs. 1 GWB.

Die Antragstellerin trägt vor, dass der Nachprüfungsantrag zulässig und begründet sei. Das Angebot der Antragstellerin enthalte inhaltlich auch unter Berücksichtigung des Betriebskonzepts Cloud-Service keine unzulässige Änderung an den Vergabeunterlagen. Der von der Antragstellerin angebotene Cloud-Betrieb werde ausschließlich in Rechenzentren in Deutschland stattfinden. Die Antragstellerin habe sowohl die Vorgaben aus den Vergabeunterlagen als auch die geltenden Datenschutzbestimmungen, insbesondere die der DSGVO eingehalten. Dies werde auch durch die zwischen der M… Ltd. und der Antragstellerin im Auftragsfall zu schließenden Zusatzvereinbarung sowie durch die sogenannte „Defending your Data“ Erklärung der M… Corporation bestätigt.
Weiter trägt die Antragstellerin vor, dass sie bestreite, dass die Vergabeunterlagen Vorgaben oder Verweise enthielten, gemäß denen ein Bieter besondere Maßnahmen zu ergreifen habe um alle erdenklichen Auskunftsbegehren oder Herausgabeverlangen von Drittsaaten, insbesondere der USA zu unterbinden. Es handle sich bei einem drittstaatlichen Auskunftsersuchen gerade nicht um einen Fall des Art. 44 DSGVO. Die Übermittlung als Unterfall der Verarbeitung verlange ein wie auch immer geartetes bewusstes, aktives Tun. Die Möglichkeit einer Zugriffsmöglichkeit durch drittstaatliche Behörden stelle aber kein bewusstes, aktives Tun dar.
Die Antragstellerin habe in ihrem Angebot zudem ein eindeutiges und klares Leistungsversprechen gemacht und versichert, dass sie die Vorgaben in den Vergabeunterlagen einhalten werde. Es seien keine konkreten Anhaltspunkte ersichtlich, dass die Antragstellerin diese nicht werde einhalten können, insbesondere habe die Antragstellerin dargelegt, dass sie alle datenschutzrechtlichen Vorgaben einhalten werde. Ferner habe die Antragstellerin auch technische Maßnahmen ergriffen um die Daten des Antragsgegners gerade vor einem drittstaatlichen Auskunftsbegehren zu schützen in dem sie die Daten verschlüsselt. Dabei verbleibe der für die Entschlüsselung notwendige Schlüssel beim Antragsgegner. Auf die von der Antragstellerin gewählte Verschlüsselungstechnik in Form des A… Key Vaults und der A… Lockbox gehe der Antraggegner bei der Begründung des Ausschlusses der Antragstellerin überhaupt nicht ein, auch die Stellungnahme des Bayerischen Landesbeauftragten für den Datenschutz berücksichtige diese technischen Maßnahmen nicht. Die Stellungnahme des Bayerischen

Landesbeauftragten für den Datenschutz sei auch zu einem Zeitpunkt erfolgt, als noch nicht alle Eingaben der Antragstellerin erfolgt waren und außerdem habe der Landesbeauftragte lediglich eine kurze Zusammenfassung des Sachverhalts vom Antragsgegner erhalten. Die Stellungnahme gehe also von einem unvollständigen Sachverhalt aus. Deshalb habe der Landesbeauftragte wohl auch die von der Antragstellerin ergriffenen technischen Maßnahmen fehlerhaft bewertet. Der Ausschluss könne und dürfe nicht auf diese Stellungnahme gestützt werden.

Der Antragsgegner habe auch in den Vergabeunterlagen keine Vorgaben gemacht, dass jedwede Speicherung von Daten in der Cloud nur verschlüsselt erfolgen müsse. Zwar würden die Daten während der Verarbeitung kurzzeitig unverschlüsselt in der Cloud vorliegen, M… müsste jedoch mit erheblichen personellen Ressourcen und gänzlich vertrags- und rechtswidrig die Cloud überwachen um den genauen Zeitpunkt zu ermitteln, an dem die Daten kurzzeitig unverschlüsselt vorliegen um diese dann abgreifen zu können. Dies sei mit vertretbarem Aufwand nicht umsetzbar. Es sei bereits fraglich, ob der Cloud-Akt überhaupt Anwendung fände, aber selbst wenn dies der Fall wäre, was die Antragstellerin bestreitet, wäre die M… Ltd. als Cloud-Provider der Antragstellerin lediglich in der Lage auf verschlüsselte Daten des Antragsgegners zuzugreifen, so dass jegliches Auskunftsersuchen im Rahmen des Cloud-Acts ins Leere laufen würden. Auch sei zu beachten, dass die Beigeladene selbst mehrere Niederlassungen in den USA habe, so dass im Falle der Anwendbarkeit des Cloud-Acts auch die Beigeladene davon betroffen wäre.

Die Antragstellerin beantragt

1. Das Nachprüfungsverfahren gemäß § 160 Abs. 1 GWB einzuleiten und
2. Dem Antragsgegner zu untersagen, den Zuschlag auf das Angebot des Bieters A… GmbH zu erteilen,
3. Akteneinsicht gemäß § 165 Abs. 1 GWB zu gewähren,
4. Auszusprechen, dass die Hinzuziehung eines Verfahrensbevollmächtigten für die Antragstellerin notwendig gewesen ist.

Der Antragsgegner beantragt

1. Der Nachprüfungsantrag der Antragstellerin vom 08. August 2022 wird als teilweise unzulässig verworfen und im Übrigen als unbegründet zurückgewiesen.
2. Die Antragstellerin trägt die Kosten des Verfahrens und die zur zweckentsprechenden Rechtsverteidigung notwendigen Aufwendungen des Antragsgegners.
3. Die Hinzuziehung eines Verfahrensbevollmächtigten durch den Antragsgegner wird für notwendig erklärt.

Zur Begründung trägt der Antragsgegner vor, dass der Ausschluss des Angebots der Antragstellerin rechtmäßig erfolgt sei. Der Antragsgegner habe den Ausschluss zum einen auf einen Verstoß gegen die Vorgaben der DSGVO und zum anderen auf einen Verstoß gegen die Anforderungen zum Ort der Leistungserbringung gestützt. Die Gefahr der Offenlegung von Daten durch ein drittstaatliches Auskunftsersuchen widerspreche den Anforderungen zum Leistungsort und sei als Datenverarbeitung zu qualifizieren. Der Antragsgegner habe in den Vergabeunterlagen eindeutig, klar und abschließend definiert, dass jegliche Datenverarbeitung zumindest im Europäischen Wirtschaftsraum erfolgen müsse. Jeder durchschnittliche Bieter habe diese Anforderungen aus den Vergabeunterlagen insbesondere im Zusammenhang mit den Antworten auf die Bieterfragen auch so verstehen müssen. Die von der Antragstellerin getroffenen organisatorischen und technischen Maßnahmen seien bei Nutzung von US-Diensten nicht ausreichend um die Anforderungen der Vergabeunterlagen zu erfüllen.
Bei den Anforderungen an die Prüfung eines Angebotes richte sich der Prüfungsumfang an die Zumutbarkeit, dies gelte auch für die Umsetzbarkeit eines angebotenen Konzepts. Bei der Prüfung des Konzepts der Antragstellerin hat der Antragsgegner das hauseigene zuständige Fachreferat sowie den Bayerischen Landesbeauftragten für den Datenschutz als zuständige Aufsichtsbehörde einbezogen. Der Antragsgegner habe alles im Rahmen seiner Möglichkeiten zumutbare unternommen um die streiterhebliche Rechtsfrage aufzuklären und zu prüfen. Der Antragsgegner habe eine datenschutzrechtlich vertretbare Entscheidung getroffen und den Angebotsausschluss darauf gestützt. Die Entscheidung des Antragsgegners sei also vergaberechtlich fehlerfrei erfolgt. Zudem sei der Bayerische Landesbeauftragte die gesetzlich zuständige Behörde für den Antragsgegner. Dass das Bayerische Landesamt für Datenschutzaufsicht als zuständige Behörde für die Antragstellerin eine andere Rechtsauffassung habe, sei bedauerlich und der aktuell unsicheren Rechtslage geschuldet, für die Bewertung des Angebots der Antragstellerin für den Antragsgegner jedoch unerheblich, da der Antragsgegner an die Anweisungen des Bayerischen Landesbeauftragten für den Datenschutz gebunden sei. Es sei ferner kein vergaberechtlicher Verstoß, dass die Antragstellerin aufgrund einer fachrechtlich ungeklärten und höchst umstrittenen Datenschutzproblematik aus dem Vergabeverfahren ausgeschlossen werden müsse. Der Antragsgegner habe im Rahmen der Angebotsprüfung und Angebotsaufklärung zwar feststellen können, dass die Antragstellerin alle technischen und vertraglichen Möglichkeiten zur Datenverschlüsselung ausgeschöpft habe, die Frage, ob diese Maßnahmen ausreichend seien um jegliche Verarbeitung von personenbezogenen Daten in Drittländern gänzlich ausschließen zu können, sei für den Fall eines erzwungenen Datenzugriffs jedoch nicht ausreichend beantwortet worden. Die Verschlüsselung durch den Lockbox-Mechanismus reiche nicht aus und für die Nutzung des A…-Key-Vaults habe die Antragstellerin nicht dargelegt, wie dieser vor einem gegebenenfalls erzwungenen Zugriff durch Drittstaaten die Daten des Antragsgegners schützen würde. Der Cloud-Provider habe Zugriff auf den Schlüssel, um während der Datenverarbeitung die Daten

zu ver- bzw. entschlüsseln, so dass diese Daten dann, wenn auch gegebenenfalls nur kurzzeitig, in unverschlüsselter Form vorlägen.
Der Antragsgegner argumentierte weiter, dass der Cloud-Act auf die geplante Auftragsdurchführung der Antragstellerin Anwendung fände, da die M… Ltd. eine Tochtergesellschaft eines US-Unternehmens sei und die USA damit auch Zugriff auf Daten, die in europäischen Rechenzentren gespeichert seien, Zugriff habe. Diese Möglichkeit der Offenlegung von personenbezogenen Daten stelle ein relevantes Risiko dar und sei eine Übermittlung im Sinne von Art. 44 DSGOV. Der Antragsgegner könne nicht mit hinreichender Sicherheit ausschließen, dass die US-amerikanischen Sicherheitsbehörden Zugriff auf die personenbezogenen Daten des Antragsgegners in unverschlüsselter Form haben könnten. Ferner habe der Antragsgegner die Antragstellerin auch nicht diskriminierend behandelt. Die Beigeladene und die Antragstellerin haben unterschiedliche Angebote mit unterschiedlichen Cloud-Providern abgegeben und seien deshalb unterschiedlich zu behandeln gewesen. Insbesondere habe die Beigeladene dargelegt, dass weder der von ihr angebotene Cloud-Provider noch ein Unterauftragnehmer einen US-Bezug hätten, sondern rein deutsche Unternehmen seien. Der Antragsgegner habe daher keine Anhaltspunkte für datenschutzrechtliche Bedenken hinsichtlich des Angebots der Beigeladenen feststellen können und diese daher auch nicht ausschließen müssen.

Mit Beiladungsbeschluss vom 05.09.2022 wurde die Beigeladene beigeladen und beantragt

1. Den Nachprüfungsantrag zurückzuweisen;
2. Hilfsweise das Verfahren in den Stand vor Angebotsabgabe zurück zu versetzen;
3. Die Kosten des Verfahrens und die zur zweckentsprechenden Rechtsverfolgung erforderlichen Aufwendungen der Beigeladenen gemäß § 182 Abs. 4 GWB der Antragstellerin aufzuerlegen;
4. Die Hinzuziehung von Verfahrensbevollmächtigten durch die Beigeladene für notwendig zu erklären.

Die Beigeladene trägt vor, dass sie selbst nach den Vergabeunterlagen und den Antworten auf die Bieterfragen erkannt habe, dass sie die ihr ebenfalls bekannte, von der Antragstellerin verwendete Cloud-Plattform … A… nicht verwenden könne und daher nicht mit dieser wesentlich kostengünstigeren Lösung anbieten dürfe. Neben dem Risiko eines drittstaatlichen Zugriffs im Rahmen des Cloud-Acts komme bei der … A… Plattform hinzu, dass in der Regel Leistungen im Zuge der Cloud-Maintenance außerhalb der Europäischen Union und des Europäischen Wirtschaftsraums erbracht würden.
Die Muttergesellschaft der Beigeladenen selbst mit Sitz in Irland unterliege, nachdem sie keine in den USA ansässige Konzernmuttergesellschaft habe nicht dem Anwendungsbereich des Cloud-Acts, ein drittstaatlich erzwungener Zugriff auf Daten des Antragsgegners sei also

ausgeschlossen. Auch der von der Beigeladenen benannte Clouddienstleister habe keinen drittstaatlichen Bezug, da er ausschließlich Sitze in Deutschland habe.

Mit rechtlichem Hinweis vom 12.09.2022 wies die Vergabekammer die Parteien auf den Beschluss des OLG Karlsruhe vom 07.09.2022 – 15 Verg 8/22 hin und bat um Stellungnahme, ob der Antragsgegner angesichts dieser neuen obergerichtlichen Rechtsprechung den Ausschluss der Antragstellerin überdenken werde und gegebenenfalls dem Nachprüfungsantrag abhelfen werde.

In der mündlichen Verhandlung vom 14.02.2023 wurde die Sach- und Rechtslage erörtert. Die Verfahrensbeteiligten hatten Gelegenheit zum Vortrag und zur Stellungnahme. Zunächst erklärten die Parteien, dass die Frage, ob die Einhaltung der DSGVO wirksam in den Vergabeunterlagen gefordert gewesen sei, unstreitig geworden sei.
Auf Nachfrage der Vergabekammer erklärte der Antragsgegner, dass er mit seiner Formulierung in den Vergabeunterlagen zum Ort der Leistungserbringung keine Konzernverflechtungen von vornherein habe ausschließen wollen. Er habe lediglich festlegen wollen, dass die konkrete Leistungserbringung in der Europäischen Union bzw. im Europäischen Wirtschaftsraum zu erfolgen habe. Er habe einen größtmöglichen Schutz der hochsensiblen Gesundheitsdaten fordern und insbesondere einen Datenabfluss in die USA verhindern wollen. Die Intention sei es gewesen, bereits gar nicht in den Anwendungsbereich des Art. 44 DSGVO zu kommen.
Die Antragstellerin erklärte, dass sie die im Ausschlussschreiben vom Antragsgegner genannten Ausschlussgründe für falsch halte. Sie habe ausführlich dargelegt, dass der Cloud-Act nicht anwendbar sei. Ferner handle es sich bei Anfragen im Rahmen des Cloud-Acts auch nicht um eine Datenverarbeitung im Sinne des Art. 44 DSGVO, dies sei auch durch den Beschluss der Datenschutzkonferenz vom 31.01.2023 bestätigt worden. Außerdem seien die Daten auch im Falle eines Auskunftsersuchens nur in verschlüsselter Form gespeichert, weshalb ein solches Ersuchen ins Leere laufen würde.
Die Beteiligten diskutierten, ob die von der Antragstellerin ergriffenen technischen Maßnahmen ausreichen würden, um die Daten in der TNA-Cloud vor drittstaatlichen Zugriffen insbesondere in Form von Auskunftsersuchen im Rahmen des Cloud-Acts zu schützen. Nachdem die technischen Experten die technischen Maßnahmen der Antragstellerin, insbesondere den A…-Key-Vault und dessen Verwendung erklärt hatten, erklärte der Antragsgegner, dass er zwar zustimme, dass der Schlüssel sicher verwahrt werde, aber M… im Zeitpunkt der Verarbeitung Zugriff auf unverschlüsselte Daten habe. Die Antragstellerin stimmte zu, dass M… im Zeitpunkt der Verarbeitung theoretisch auf unverschlüsselte Daten zugreifen könnte, dass es sich dabei aber nur um wenige Millisekunden handle. Auch würde M… die Ver- und Entschlüsselung nicht selbst handhaben und habe im Zweifel nur Zugriff auf die zufällig gerade verwendeten und aus diesem Grund unverschlüsselt vorliegenden Daten. Der Antragsgegner erklärte, dass diese

zufälligen Datensätze mitunter sehr umfangreich seien und eine Vielzahl von hochsensiblen Daten enthalten könnten.
Bezüglich des Schreibens des Datenschutzbeauftragten vom 15.07.2022 wurde der Antragsgegner gefragt, weshalb er nicht bezüglich einer fehlenden Aussage zur Verschlüsselung und der Verwendung des A… Key Vault nachgefragt habe, nachdem die Auskunft des Datenschutzbeauftragten hierauf nicht eingegangen sei. Der Antragsgegner erklärte dazu, dass für ihn die Sachlage klar gewesen sei und man eine weitere schriftliche Antwort des Datenschutzbeauftragten nicht mehr für nötig gehalten habe, insbesondere nach der fernmündlichen Androhung aufsichtsrechtlicher Konsequenzen durch den Datenschutzbeauftragten. Der Antragsgegner habe sich hier gebeugt, und die sichere Lösung gewählt, da er es nicht auf aufsichtsrechtliche Konsequenzen ankommen lassen wollte. Zudem habe er sich umfassend und tiefgreifend mit allen ermittelten Erkenntnissen auseinandergesetzt und in einer großen Runde mit allen Fachstellen diskutiert und abgewogen. Er habe sich auf dieser Grundlage für die risikofreie Lösung entschieden und keine einseitige oder politisch motivierte Entscheidung getroffen. Auf die Frage nach einer Dokumentation dieser Gesprächsrunde erklärte der Antragsgegner, dass es keine gebe, man habe das interne Gespräch nicht protokolliert, sondern lediglich das Ergebnis der Vergabestelle mitgeteilt.

Der ehrenamtliche Beisitzer hat die Entscheidung über die Beiladung, den Umfang der Akteneinsicht sowie im Falle einer Verfahrenseinstellung auf die Vorsitzende und die hauptamtliche Beisitzerin übertragen.

Die Beteiligten wurden durch den Austausch der jeweiligen Schriftsätze informiert. Auf die ausgetauschten Schriftsätze, das Protokoll der mündlichen Verhandlung, die Verfahrensakte der Vergabekammer sowie auf die Vergabeakten, soweit sie der Vergabekammer vorgelegt wurden, wird ergänzend Bezug genommen.

II.

1. Der Nachprüfungsantrag ist statthaft und zulässig.

1.1. Die Vergabekammer Südbayern ist für die Überprüfung des streitgegenständlichen Vergabeverfahrens zuständig. Die sachliche und örtliche Zuständigkeit der Vergabekammer Südbayern ergibt sich aus §§ 155, 156 Abs. 1, 158 Abs. 2 GWB i. V. m. §§ 1 und 2 BayNpV.
Gegenstand der Vergabe ist ein Dienstleistungsauftrag i. S. d. § 103 Abs. 4 GWB. Der Antragsgegner ist Auftraggeber gemäß §§ 98, 99 Nr. 1 GWB. Der geschätzte Gesamtauftragswert überschreitet den gemäß § 106 GWB maßgeblichen Schwellenwert.

Eine Ausnahmebestimmung der §§ 107 - 109 GWB liegt nicht vor.

1.2. Die Antragstellerin ist auch antragsbefugt.
Gemäß § 160 Abs. 2 GWB ist ein Unternehmen antragsbefugt, wenn es sein Interesse am Auftrag, eine Verletzung in seinen Rechten nach § 97 Abs. 6 GWB und zumindest einen drohenden Schaden darlegt. Die Antragstellerin hat ihr Interesse am Auftrag durch die Abgabe eines Angebots nachgewiesen. Es ist nicht erkennbar, dass sie mit diesem Nachprüfungsantrag einen anderen Zweck verfolgt, als den, den strittigen Auftrag zu erhalten. Die Antragstellerin hat eine Verletzung in ihren Rechten nach § 97 Abs. 6 GWB insbesondere durch den Ausschluss ihres Angebots geltend gemacht.

1.3. Der Zulässigkeit des Nachprüfungsantrags steht auch keine Rügepräklusion nach § 160 Abs. 3 S. 1 Nr. 1 GWB entgegen, da die Antragstellerin den Ausschluss ihres Angebots wegen Verstoßes gegen die Vorgaben der Leistungsbeschreibung mit Schreiben vom 03.08.2022 innerhalb der gesetzlichen Frist von 10 Kalendertagen gerügt hat.

2. Der Nachprüfungsantrag ist auch begründet.
Die Antragstellerin ist durch den Ausschluss ihres Angebots in ihren Rechten verletzt, § 168 Abs. 1 Satz 1 GWB. Der Antragsgegner kann derzeit nicht nachweisen, dass die Voraussetzungen des § 57 Abs. 1 Nr. 4 VgV vorliegen und hat auf Grundlage einer unzureichenden Prüfung der von der Antragstellerin angebotenen technischen Maßnahmen angenommen, dass das Angebot der Antragstellerin gegen die Art. 44 ff. DSGVO und damit die Vorgaben der Leistungsbeschreibung verstößt. Die bisher vom Antragsgegner durchgeführte Prüfung des Angebots der Antragstellerin berücksichtigt angebotene technische Maßnahmen, die einen Zugriff von Drittstaaten auf unverschlüsselte personenbezogene Daten verhindern sollen, nicht ordnungsgemäß. Zudem ist aus der vom Antragsgegner vorgelegten Dokumentation nicht ersichtlich, ob er sich ausreichend mit der Frage auseinandergesetzt hat, ob und inwieweit ein Risiko für etwaige drittstaatliche Auskunftsbegehren gegenüber dem Cloud-Provider überhaupt besteht, wenn zufällig personenbezogene Daten für kurze Zeit unverschlüsselt in der Cloud vorliegen.

2.1. Der Antragsgegner hat den Ausschluss des Angebots der Antragstellerin einerseits auf einen Verstoß gegen die Vorgaben der DSGVO und andererseits auf einen Verstoß gegen die Anforderungen zum Ort der Datenverarbeitung und zum Ort der Leistungserbringung gestützt.

Hinsichtlich des Ortes der Leistungserbringung hat der Antragsgegner in den Vergabeunterlagen lediglich die geplante, vertragsgemäße Leistungserbringung außerhalb der Europäischen Union (EU) bzw. des Europäischen Wirtschaftsraums (EWR) ausgeschlossen. Über die Einhal-

tung der einschlägigen datenschutzrechtlichen Regulierungen hinaus, hat der Antragsgegner keine Vorgaben bezüglich spezieller Schutzmaßnahmen gegenüber denkbaren Herausgabeverlangen drittstaatlicher Behörden gemacht.

2.1.1. Die Verpflichtung der Bieter, dass die Leistungserbringung unter Einhaltung der Vorgaben der DSGVO erfolgen muss, ergibt sich aus folgenden Formulierungen in den Vergabeunterlagen: „Der AN hat die Erfüllung der ihn betreffenden im Datenschutzkonzept dargestellten und regulatorischen datenschutzrechtlichen Anforderungen sicherzustellen.“ (Ziffer 2.7.1. des Lastenhefts) und „Auf der Grundlage des Konzeptes soll gewährleistet sein, dass die Leistung des Bieters den Anforderungen der datenschutzrechtlichen Regulierungen entspricht und personenbezogene Daten höchstmöglich geschützt sind.“ (Ziffer 1.3.1.6 Datenschutzkonzept). Dies war zuletzt in der mündlichen Verhandlung auch zwischen den Beteiligten unstreitig.

2.1.2. Hinsichtlich des Orts der Leistungserbringung war in den Vergabeunterlagen im Muster eines Auftragsverarbeitungsvertrags nach Art. 28 Abs. 3 DSGVO geregelt, dass der „Auftragnehmer […] die Leistungen nach diesem Vertrag ausschließlich in der Bundesrepublik Deutschland, einem Mitgliedsstaat der Europäischen Union oder einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum“ erbringt. Im Lastenheft war unter der Ziffer 4. zu dem Cloud-Service für das TNA-System unter anderem geregelt: „Ressourcen Standort und Datenverarbeitung: Europäische Union bzw. Europäischer Wirtschaftsraum (EWR)“.

Auch die Beantwortung der Bieterfrage Nr. 212, ob eine Einbeziehung europäischer Cloud Provider mit dem Hauptsitz in der Schweiz möglich ist, welche ihre Supportleistungen von dort erbringen, schließt nicht wie die Beigeladene im Schriftsatz vom 04.10.2022 vorträgt, jeglichen Bezug zu nicht EU bzw. EWR-Staaten aus. Die Antwort stellt lediglich klar, dass für die geplante Erbringung von vertragsgemäßen Leistungen nur EU- bzw. EWR Staaten in Betracht kommen, egal ob ein Angemessenheitsbeschluss für diese Drittstaaten besteht.

Der Antragsgegner bestätigt hierzu in der mündlichen Verhandlung, dass er mit den oben genannten Formulierungen im Muster eines Auftragsverarbeitungsvertrags und im Lastenheft explizit regeln wollte, dass keine geplante vertragsmäßige Leistungserbringung außerhalb der EU bzw. des EWR stattfinden soll und man somit bereits gar nicht in den Anwendungsbereich der Art. 44 ff. der DSGVO kommen würde. Zudem sollten die sensiblen persönlichen Daten bestmöglich geschützt sein, so dass ein Datenabfluss in Drittstaaten verhindert würde. Nicht gewollt dagegen sei ein Ausschluss von jeglichen Firmen mit Konzernbezug in Drittstaaten außerhalb der EU bzw. dem EWR gewesen.

2.2. Auf Grund der vom Antragsgegner bisher durchgeführten Prüfung des Angebots der Antragstellerin, ist deren Angebot nicht wegen einer Änderung der Vergabeunterlagen nach § 57 Abs. 1 Nr. 4 VgV auszuschließen. Der Antragsgegner hat es bei der Prüfung des Angebots der Antragstellerin unterlassen, die von der Antragstellerin in ihrem mit dem Angebot abgegebenen Datenschutzkonzept vorgesehenen Verschlüsselung als technische Maßnahme, um Zugriff auf die personenbezogenen Daten zu verhindern, hinreichend bei einer Beurteilung der Vereinbarkeit des Angebots mit den Vorgaben der Vergabeunterlagen zu berücksichtigen.

Gem. § 56 Abs. 1 VgV sind Angebote auf Vollständigkeit sowie fachliche und rechnerische Richtigkeit zu prüfen. Die fachliche Richtigkeitsprüfung der Angebote bezieht sich auf den fachlichen Inhalt der von den Bietern eingereichten Unterlagen und umfasst regelmäßig die Prüfung, ob die angebotene Leistung den Anforderungen der Ausschreibung, insbesondere der Leistungsbeschreibung und den technischen Spezifikationen entspricht. (vgl. Beck VergabeR/Haak/Hogeweg, 3. Aufl. 2019, VgV § 56 Rn. 23). Ein öffentlicher Auftraggeber ist zwar grundsätzlich nicht verpflichtet zu überprüfen, ob die Bieter ihre mit dem Angebot verbindlich eingegangenen vertraglichen Verpflichtungen auch einhalten werden; vielmehr darf er sich grundsätzlich auch ohne Überprüfung auf die Leistungsversprechen der Bieter verlassen (OLG Düsseldorf, Beschluss vom 15.01.2020 - Verg 20/19 m. w. N.; OLG Karlsruhe, Beschluss vom 29.05.2020 - 15 Verg 2/20). Entscheidet sich ein öffentlicher Auftraggeber jedoch dazu, das Leistungsversprechen des Bieters zu überprüfen, muss der öffentliche Auftraggeber aus Gründen der Transparenz und der Gleichbehandlung der Bieter bereit und in der Lage sein, das Leistungsversprechen des Bieters effektiv zu verifizieren (OLG Düsseldorf, Beschluss vom 15.01.2020 - Verg 20/19).

2.2.1. Der öffentliche Auftraggeber ist in der Wahl seiner Überprüfungsmittel grundsätzlich frei (OLG München, Beschluss vom 11.05.2007 - Verg 4/07; OLG Frankfurt a.M. Beschluss vom 16.06.2015 - 11 Verg 3/15 - zur Eignungsbeurteilung). Er ist im Interesse einer zügigen Umsetzung der Beschaffungsabsicht und einem raschen Abschluss des Vergabeverfahrens und aus Gründen seiner begrenzten Ressourcen und administrativen Möglichkeiten nicht auf eine bestimmte Methode oder bestimmte Mittel der fachlichen Prüfung festgelegt. Die vorgenannten Maßstäbe gelten gleichermaßen für die zu fordernde Prüfungstiefe in Fällen, in denen die Prüfung, ob ein Angebot den Anforderungen der Vergabeunterlagen entspricht und ob die angebotenen Konzepte umsetzbar sind, die Beurteilung einer Vielzahl komplexer technischer Fragen erfordert. (OLG Düsseldorf, Beschluss vom 05.07.2012 - Verg 13/12). Das vom Auftraggeber gewählte Mittel zur Überprüfung muss jedoch geeignet und die Mittelauswahl frei von sachwidrigen Erwägungen getroffen worden sein (OLG Düsseldorf, Beschluss vom 15.01.2020 - Verg 20/19).

Gegen die vom Antragsgegner herangezogenen Erkenntnisquellen für die Beurteilung der fachlichen Richtigkeit und der Übereinstimmung des Angebots der Antragstellerin mit den Vorgaben der Vergabeunterlagen hinsichtlich der Einhaltung der datenschutzrechtlichen Anforderungen hat die Vergabekammer keine grundlegenden Bedenken.

Der Antragsgegner hat im Rahmen der fachlichen Prüfung einen IT-Beschaffungsdienstleister, dessen externen Datenschutzbeauftragten, das zuständige Sachgebiet für Datenschutz im Bayerischen Staatsministerium des Inneren, für Sport und Integration, den Bayerischen Landesbeauftragten für den Datenschutz und die zum Entscheidungszeitpunkt verfügbare einschlägige Rechtsprechung einbezogen.
Der Antragsgegner trägt in seinem Schriftsatz vom 31.08.2022 vor, dass keine weiteren Möglichkeiten einer Überprüfung, die in einem Vergabeverfahren durchgeführt werden könnten, sowie angemessen und zumutbar gewesen wären, ersichtlich seien. Die Vergabekammer folgt der Auffassung insoweit, dass dem Antragsgegner damit eine ausreichende Auswahl an Prüfmöglichkeiten zur Verfügung gestanden hat, welche er für die Beurteilung der fachlichen Richtigkeit heranziehen konnte. Dass der Antragsgegner keine (weiteren) Gutachten von Sachverständigen eingeholt hat, ist an sich nicht zu beanstanden, da die vom Antragsgegner getroffene Auswahl der Überprüfungsmöglichkeiten wohl grundsätzlich geeignet gewesen wäre, die fachliche Richtigkeit des Angebots der Antragstellerin und eine Übereinstimmung mit den Vorgaben der Vergabeunterlagen zu beurteilen.

2.2.2. Der Antragsgegner hat sich bei der Prüfung der Frage, ob bei drittstaatlichen Auskunftsbegehren hinsichtlich der Daten, die mit der von der Antragstellerin angebotenen Verschlüsselungsmethode verschlüsselt sind und die in der von der Antragstellerin angebotenen Cloud-Lösung gespeichert werden, ein Verstoß gegen die Vorgaben der Vergabeunterlagen, nämlich die Einhaltung der datenschutzrechtlichen Bestimmungen, vorliegt, nicht ausreichend mit der von der Antragstellerin angebotenen Verschlüsselungsmethode als technische Maßnahme befasst.
Der Antragsgegner hat es dabei bereits versäumt, seine Fragen hinsichtlich der von der Antragstellerin eingesetzte Verschlüsselungsmethode ordnungsgemäß aufzuklären. Insbesondere auf Grund der völlig fehlenden Dokumentation der getroffenen Entscheidung ist auch nicht ersichtlich, dass der Antragsgegner alle ihm vorliegenden Erkenntnisse in seine Entscheidungsfindung eingestellt hat. Die der Vergabekammer vorliegende Dokumentation deutet vielmehr darauf hin, dass die Entscheidung sich wesentlich auf die Einschätzung des Bayerischen Landesbeauftragten für Datenschutz stützt, welche sich mit der Thematik der Verschlüsselung überhaupt nicht befasst.

Bereits am 27.04.2022 hat der IT-Beschaffungsdienstleister per E-Mail zu dem von der Antragstellerin mit dem Angebot eingereichten Datenschutzkonzept folgende Stellungnahme seines externen Datenschutzbeauftragten übermittelt: „Kernargument ist aus meiner Sicht die durchgängige technische Verwendung einer Verschlüsselung mit kundenseitigem Schlüssel (Bring Your Own Key, „BYOK“) der Daten in den relevanten Teilsystemen, die in den meisten Fällen auch noch ergänzt wird um eine zusätzliche Verschlüsselung durch den RZ-Betreiber. Dies führt aus meiner Sicht dazu, dass bei einem theoretischen Zugriff unberechtigter Dritter (z.B. durch US-Sicherheitsbehörden mittels einer erzwungenen Bereitstellung via M… -> M…) zwar technisch Daten aus Deutschland in die USA übertragen würden, diese aber auf Grund ihrer Verschlüsselungsart (BYOK) für die Dritten nicht entschlüsselbar wären und somit kein faktischer Zugriff auf personenbeziehbare / personenbezogene Daten möglich ist.“

Auf die vom Auftraggeber in einer E-Mail vom 27.04.2022 geäußerten Bedenken, dass der Cloud-Anbieter Zugriff auf den Schlüssel haben könnte, da die Daten in der Cloud ver- und entschlüsselt würden und damit der Schlüssel ebenfalls in der Cloud gespeichert würde, antwortete der externe Datenschutzbeauftragte des IT-Beschaffungsdienstleisters in einer E-Mail vom 29.04.2022, dass „die Nutzung des BYOK-Verfahrens vorgesehen [wird], bei der letztendlich eine Verarbeitung von personenbezogenen Daten in einem Drittland (inkl. Transfer dorthin) technisch verunmöglicht wird. Diese Verunmöglichung hat nach meiner Einschätzung auch Bestand, wenn der kundeneigene Key in einem A… Vault gespeichert wird, denn nach mir vorliegenden Informationen (durch einen IT-Spezialisten bestätigt) ist auch für M… selbst ein Zugang zu kundeneigenen Schlüsseln durch eine Zertifikatsabsicherung des A… Vault, bei der das Zertifikat ebenfalls vom Kunden kommt, nicht möglich.“

Der Aussage, dass auch für M… selbst ein Zugang zu dem kundeneigenen Schlüssel im A… Key Vault nicht möglich ist, schloss sich der Antragsgegner in der mündlichen Verhandlung schließlich auch an.

Der Antragsgegner war in einer internen E-Mail vom 02.05.2022 auch der Ansicht, dass auf Grund der Verschlüsselung insbesondere auf Grund der Verwendung eines Kundenschlüssels, durchaus die Möglichkeit bestehe, den verschlüsselten Daten den Personenbezug abzusprechen und dass daher das Angebot der Antragstellerin in dieser Hinsicht weiter aufgeklärt werden müsse.

Im Rahmen einer Angebotsaufklärung hat der öffentliche Auftraggeber an den Bieter eine eindeutig formulierte Anforderung zu richten, mit der er die Erläuterung bestimmter unklarer Punkte im Angebot verlangt (vgl. OLG Düsseldorf, Beschluss vom 29.05.2020 - Verg 26/19 zur Preisaufklärung). Der Antragsgegner hat dagegen zu der Problematik der Verschlüsselung als

Schutz gegen Auskunftsbegehren von Drittstaaten in seiner Bitte um Aufklärung an die Antragstellerin vom 05.05.2022 keine konkreten Fragen gestellt, sondern stattdessen ein abstraktes Szenario gezeichnet, in welchem bei einer in einem Drittland stattfindenden Datenverarbeitung „in einer zweiten Variante“ die Verarbeitung personenbezogener Daten nicht vorläge, wenn alle Daten im Zugriffsbereich des Drittlandes so verarbeitet werden, dass eine Personenbeziehbarkeit ausgeschlossen ist bzw. werden kann. Der Antragsgegner teilte der Antragstellerin im Aufklärungsschreiben dann lediglich noch mit, dass für die „zweite Variante“ „auch eine interne Verschlüsselung der Datenverarbeitung und Datenablage mit einem nutzereigenen Schlüssel keine hinreichende Gewähr für einen Schutz gegen etwaige Einsichtnahmen in die Daten bietet bzw. zu bieten vermag, da im cloud-System selbst personenbezogene Daten verarbeitet werden. Dies setzt technisch eine Entschlüsselung der Daten im Zugriffsbereich des Cloud-Betreibers voraus.“ Schließlich teilt der Antragsgegner noch mit, dass „zudem […] der verwendete Nutzerschlüssel ebenfalls auf Komponenten in der cloud-Infrastruktur abgelegt [werde]“.

Die Antragstellerin durfte dieses ohne konkrete Aufklärungsfragen verfasste Schreiben des Antragsgegners hinsichtlich der geschilderten „zweiten Variante“ so verstehen, als dass der Antragsgegner davon ausgeht, dass sie mit der Cloud-Lösung eine geplante Datenverarbeitung in einem Drittstaat anbiete. Dass mit der Formulierung „im Zugriffsbereich eines Drittstaates“ auch die Möglichkeit etwaiger drittstaatlicher Auskunftsbegehren gemeint sein sollte, ist nur nachvollziehbar, wenn die vorherige interne Diskussion per E-Mail um diese Frage bekannt ist. Diese interne Diskussion des Antragsgegners kannte die Antragstellerin jedoch nicht. Daher erläuterte sie in ihrem Antwortschreiben vom 11.05.2022 auch ausführlich, dass keine geplante Datenverarbeitung in Drittländern stattfindet und wie sie dies sicherstellen würde. Dass die Antragstellerin in der Aufklärung jedoch die „kritische Fragestellung, ob die Nutzung der technischen und vertraglichen Maßnahmen in der A…-Cloud ausreichend ist, um die Verarbeitung von personenbezogenen Daten in Drittländern (bei erzwungenem Datenzugriff) gänzlich ausschließen zu können“ unbeantwortet ließ, wie der Antragsgegner dann in seinem Schreiben an den Bayerischen Landesbeauftragten für den Datenschutz vom 17.05.2022 monierte, lag daran, dass der Antragsgegner es im Aufklärungsverlangen versäumt hat, diese für ihn als essentiell erkannte Frage auch klar und unmissverständlich zu stellen.

Der Antragsgegner hat letztlich seine Einstufung des Angebots der Antragstellerin als nicht den Vorgaben der Vergabeunterlagen entsprechend maßgeblich auf den Aspekt gestützt, „dass wir die regulatorischen und politischen Risiken für nicht tragbar halten, die sich aus einer Vergabe entgegen einer Bewertung des für uns zuständigen BayLfD ergeben“, wie in der internen E-Mail vom 20.07.2022 dokumentiert. Der Antragsgegner hat dabei jedoch nach der der Vergabekammer vorliegenden Dokumentation vollständig unberücksichtigt gelassen, dass der Bayerische Landesbeauftragte für den Datenschutz in seinem Schreiben vom 17.05.2022

keinerlei Aussagen zu der von der Antragstellerin geplanten Verschlüsselungsmethode und dem Einsatz des A… Key Vault getroffen hat. Diese Thematik wurde in diesem Schreiben nicht erwähnt. Soweit der Antragsgegner in der mündlichen Verhandlung erklärte, er sei der fehlenden Aussage zu diesem Themenkomplex nicht weiter nachgegangen, da für ihn die Sachlage damit klar gewesen sei, kann dem nicht gefolgt werden. Dem Antragsgegner war bewusst, dass diese Frage entscheidend für die Beurteilung des Angebots der Antragstellerin war, wie die im Vorfeld der Angebotsaufklärung und Anfrage an den Bayerischen Landesbeauftragten für den Datenschutz geführte interne Korrespondenz belegt. Für eine ordnungsgemäße Beurteilung des Angebots der Antragstellerin hätte der Antragsgegner daher diesbezüglich entweder beim Bayerischen Landesbeauftragten für den Datenschutz explizit noch einmal bezüglich der Thematik Verschlüsselung und A… Key Vault nachfragen müssen oder aber eine eigene Bewertung dieser Frage vornehmen und dokumentieren müssen. Das Schreiben des Bayerischen Landesbeauftragten für den Datenschutz vom 20.05.2022 hätte für eine eigenständige Beurteilung der Verschlüsselung und des A… Key Vaults mit der Formulierung, dass „effektive zusätzliche Maßnahmen“ zu prüfen seien, diese Möglichkeit durchaus eröffnet. Der Antragsgegner hat jedoch intern wie auch im Schreiben nach § 134 GWB vom 29.07.2022 der Antragstellerin gegenüber den Ausschluss des Angebots maßgeblich auf die Beurteilung des Bayerischen Landesbeauftragten für den Datenschutz vom 20.05.2022 gestützt, obwohl dieser erkennbar zu dem für eine Beurteilung essentiellen Punkt der Verschlüsselung und dem A… Key Vault keine Aussagen trifft.

Soweit der Antragsgegner in der mündlichen Verhandlung erklärt hat, dass er sich nicht ausschließlich auf die Beurteilung des Bayerischen Landesbeauftragten für den Datenschutz vom 20.05.2022 gestützt habe, sondern sich umfassend und tiefgreifend mit allen ermittelten Erkenntnissen auseinandergesetzt und in einer großen Runde mit allen Fachstellen diskutiert und abgewogen habe, ist eine hinreichende Dokumentation hierzu nicht vorhanden. Eine derartige Dokumentation wäre aber nach § 8 Abs. 1 Satz 1 und 2 VgV zwingend nötig gewesen, da es sich hierbei um die Dokumentation einer internen Beratung über die Gründe für die Auswahlentscheidung und die Zuschlagserteilung gehandelt hat. Die Dokumentation muss alle Informationen enthalten, die notwendig sind, um die Entscheidungen des öffentlichen Auftraggebers nachvollziehen zu können (vgl. OLG Schleswig, Beschluss vom 27.10.2022 – 54 Verg 7/22; vgl. Fett in: BeckOK Vergaberecht, Stand 31.01.2023, § 8 VgV, Rn. 19). Hierfür muss ein öffentlicher Auftraggeber seine für die Zuschlagserteilung maßgeblichen Erwägungen in allen Schritten so eingehend dokumentieren, dass nachvollziehbar ist, ob der öffentliche Auftraggeber den Sachverhalt umfassend ermittelt hat, welche Aspekte er letztlich bei seiner Entscheidung berücksichtigt hat, welches Gewicht er ihnen zugemessen hat und was seine tragenden Argumente für die Entscheidung waren. Diese vom BGH im Beschluss vom 04.04.2017 (Az.: X ZB 3/17) für die Dokumentation der Wertungsentscheidung entwickelten Grundsätze sind auch

auf andere dokumentationspflichtige Entscheidungen des öffentlichen Auftraggebers anwendbar.

Die vom Antragsgegner vorgelegte interne E-Mail an die Vergabestelle vom 20.07.2022 spricht zwar auch von „vielfachen Abstimmungen und Rücksprachen“, so dass die Vergabekammer keine Anhaltspunkte dafür sieht, dass diese nicht stattgefunden hätten. In derselben E-Mail ist jedoch nur als leitender Aspekt für die Entscheidung die Bewertung des Bayerischen Landesbeauftragten für den Datenschutz erwähnt. Die Berücksichtigung und Abwägung anderer Aspekte, insbesondere der Beurteilung des externen Datenschutzbeauftragten des IT-Beschaffungsdienstleisters, bei der Entscheidungsfindung des Antragsgegners sind nirgendwo dokumentiert.

2.2.3. Der Antragsgegner hat hinsichtlich der Gefahr drittstaatlicher Zugriffsmöglichkeit auf unverschlüsselte Daten, die in der von der Antragstellerin angebotenen Cloud-Lösung gerade verwendet werden, keinerlei Erwägungen dokumentiert, inwieweit diese Frage Einfluss auf seine Entscheidungsfindung hatte. Es ist insbesondere nicht dokumentiert, ob er sich ausreichend mit der Frage auseinandergesetzt hat, ob und inwieweit ein Risiko für etwaige drittstaatliche Auskunftsbegehren gegenüber dem Cloud-Provider überhaupt besteht, wenn zufällige personenbezogene Daten für kurze Zeit unverschlüsselt in der Cloud vorliegen.

In den internen E-Mails vor dem Aufklärungsverlangen gegenüber der Antragstellerin hatte der Antragsgegner zwar die Frage angerissen, dass innerhalb der Cloud Daten entschlüsselt, verarbeitet und wieder verschlüsselt werden, dies aber stets als eine Gefahr dahingehend gesehen, dass damit der benötigte Schlüssel ebenfalls in der Cloud gespeichert werden muss und damit M… Zugriff auf den Schlüssel haben könnte. Auch im Aufklärungsschreiben an die Antragstellerin vom 05.05.2022 hatte der Antragsgegner seine Bedenken hinsichtlich der Entschlüsselung von Daten im Zugriffsbereich des Cloud-Betreibers lediglich kurz erwähnt und nicht eindeutig in den Kontext der Gefahr der drittstaatlichen Zugriffe auf während der aktuellen Verwendung unverschlüsselt vorliegenden Daten gestellt. Nicht einmal die Anfrage des Antragsgegners an den Bayerischen Landesbeauftragten für Datenschutz vom 17.05.2022 enthielt Ansatzpunkte zu diesem Problemkreis. Erst im Informationsschreiben nach § 134 GWB vom 29.07.2022 erwähnte der Antragsgegner erneut die Problematik, dass unverschlüsselte personenbezogene Daten im Zugriffsbereich des Cloud-Betreibers verarbeitet würden und stützte den Ausschluss der Antragstellerin wegen Abweichung von den Vorgaben der Vergabeunterlagen auch auf diesen Punkt.

Im Nachprüfungsverfahren berief sich der Antragsgegner schließlich im Schriftsatz vom 31.08.2022 auf Seite 37 darauf, dass aus technischer Sicht die Zugriffsmöglichkeit auf solche

Daten ebenfalls relevant sei, die während des Betriebs der Telenotarzt-Applikation gegebenenfalls auch nur kurzzeitig in unverschlüsselter Form vorliegen. Diese Bedenken führte der Antragsgegner in der mündlichen Verhandlung weiter aus und bekräftigte, dass er es für bedenklich halte, dass im Rahmen des Betriebs der Telenotarzt-Applikation in der Cloud ständig Datensätze ver- und entschlüsselt würden und somit zeitweise in unverschlüsselter Form in der Cloud vorlägen. Diese unverschlüsselt vorliegenden Datensätze seien zwar in gewisser Weise zufällig davon abhängig, dass sie gerade für die Applikation benötigt würden, könnten aber mitunter sehr umfangreich sein und eine Vielzahl von hochsensiblen personenbezogenen Daten enthalten.

Es liegt der Vergabekammer keine Dokumentation vor, ob der Antragsgegner bezüglich der kurzzeitig unverschlüsselt in der Cloud vorliegenden zufälligen personenbezogenen Daten überhaupt geprüft hat, ob hier eine Gefahr von drittstaatlichen Auskunftsbegehren hinsichtlich dieser Daten besteht und wie diese Gefahr zu bewerten ist. Insbesondere wäre hierbei zu berücksichtigen gewesen ob die vom Antragsgegner im Informationsschreiben nach § 134 GWB vom 29.07.2022 für das Risiko von Auskunftsbegehren aus den USA benannten Grundlagen, nämlich Section 702 FISA und der CLOUD Act überhaupt auf diese besondere Fallkonstellation Anwendung fänden. Es erscheint nicht ausgeschlossen, dass beide Grundlagen nicht die Herausgabe unspezifizierter, zufälligerweise in der Cloud unverschlüsselt vorhandenen personenbezogen Daten zum Ziel haben, sondern zielgerichtet die beispielsweise zu bestimmten Personen oder Unternehmen gespeicherten Daten abfragen sollen. Eine derartige Prüfung ob das Recht und die Rechtspraxis eines Drittlandes die Verpflichtungen aus dem Auftragsverarbeitungsvertrag beeinträchtigen könnte, legt beispielsweise auch die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder in ihrem Beschluss vom 31. Januar 2023 bei der Zuverlässigkeitsprüfung nach Art. 28 Abs. 1 DSGVO des Auftragsverarbeiters den Verantwortlichen auf.

3. Kosten des Verfahrens

Die Kosten des Verfahrens vor der Vergabekammer hat gemäß § 182 Abs. 3 Satz 1 GWB derjenige zu tragen, der im Verfahren vor der Vergabekammer unterlegen ist. Dies sind vorliegend der Antragsgegner und die Beigeladene. Diese haften für die Kosten gem. § 182 Abs. 2 Satz 2 GWB als Gesamtschuldner.

Die Gebührenfestsetzung beruht auf § 182 Abs. 2 GWB. Diese Vorschrift bestimmt einen Gebührenrahmen zwischen 2.500 Euro und 50.000 Euro, der aus Gründen der Billigkeit auf ein Zehntel der Gebühr ermäßigt und, wenn der Aufwand oder die wirtschaftliche Bedeutung außergewöhnlich hoch sind, bis zu einem Betrag vom 100.000 Euro erhöht werden kann.

Die konkrete Höhe der Gebühr richtet sich nach dem personellen und sachlichen Aufwand der Vergabekammer unter Berücksichtigung der wirtschaftlichen Bedeutung des Gegenstands des Nachprüfungsverfahrens. Da in diesem Fall sowohl der Auftragswert sehr hoch war und damit der Gegenstand des Nachprüfungsverfahrens eine hohe wirtschaftliche Bedeutung hatte als auch die Vergabeakten sehr umfangreich waren und das Verfahren eine Vielzahl an komplexen Rechtsthemen beinhaltet hat, ist bei der Vergabekammer auch ein erheblicher Arbeitsaufwand entstanden. Die Gebührenfestsetzung am oberen Rand des normalen Gebührenrahmens ist daher angemessen. Gründe für eine Ermäßigung der Gebühr aus Gründen der Billigkeit sind nicht ersichtlich.

Der Antragsgegner ist als Bundesland von der Zahlung der Gebühr nach § 182 Abs. 1 S. 2 GWB i. V. m. § 8 Abs. 1 Nr. 2 VwKostG (Bund) vom 23. Juni 1970 (BGBl. I S. 821) in der am 14. August 2013 geltenden Fassung befreit.

Von der Antragstellerin wurde bei Einleitung des Verfahrens ein Kostenvorschuss in Höhe von 2.500 Euro erhoben. Dieser Kostenvorschuss wird nach Bestandskraft erstattet.

Die Entscheidung über die Tragung der zur zweckentsprechenden Rechtsverfolgung notwendigen Aufwendungen der Antragstellerin beruht auf § 182 Abs. 4 S. 1 GWB.
Die Zuziehung eines anwaltlichen Vertreters wird als notwendig i. S. v. § 182 Abs. 4 S. 4 GWB i. V. m. Art. 80 Abs. 2 S. 3, Abs. 3 S. 2 BayVwVfG angesehen. Die anwaltliche Vertretung war erforderlich, da es sich bei der streitgegenständlichen Vergabe um ein aufwändiges und komplexes IT-Verfahren handelt, das neuartige Leistungen aus dem Bereich Telemedizin zum Gegenstand hat. Zudem berührt das hiesige Nachprüfungsverfahren zahlreiche komplexe Rechtsfragen aus dem Bereich des Datenschutzrechts und deren Einbeziehung in einen vergaberechtlichen Kontext. Die Antragstellerin ist als mittelständisches Unternehmen nicht darauf eingerichtet, derartig umfangreiche und tiefgreifende vergaberechtliche Probleme selbst zu bearbeiten und in einem kontradiktorischen Verfahren vor der Vergabekammer zu vertreten.

Rechtsmittelbelehrung

Gegen die Entscheidung der Vergabekammer kann binnen einer Notfrist von zwei Wochen (§ 172 GWB), die mit der Zustellung der Entscheidung beginnt, die sofortige Beschwerde (§ 171 GWB) schriftlich beim Bayerischen Obersten Landesgericht eingelegt werden. Die Briefanschrift lautet:

Bayerisches Oberstes Landesgericht

Schleißheimer Str. 141

80797 München

Die sofortige Beschwerde ist zugleich mit ihrer Einlegung zu begründen. Die Beschwerdebegründung muss enthalten:

1. Die Erklärung, inwieweit die Entscheidung der Vergabekammer angefochten und eine abweichende Entscheidung beantragt wird, und
2. die Angabe der Tatsachen und Beweismittel, auf die sich die Beschwerde stützt.

Die Beschwerdeschrift muss durch einen bei einem deutschen Gericht zugelassenen Rechtsanwalt unterzeichnet sein. Dies gilt nicht für Beschwerden von juristischen Personen des öffentlichen Rechts.
Mit der Einlegung der Beschwerde sind die anderen Beteiligten des Verfahrens vor der Vergabekammer vom Beschwerdeführer durch Übermittlung einer Ausfertigung der Beschwerdeschrift zu unterrichten.

München, 28.02.2023

Müller	Orlick	Demharter
Vorsitzende	Hauptamtliche Beisitzerin	Ehrenamtlicher Beisitzer