Der Bayerische Landesbeauftragte
für den Datenschutz

Datenschutz als Kriterium im Vergabeverfahren

Orientierungshilfe

Herausgeber:

Der Bayerische Landesbeauftragte für den Datenschutz
80538 München | Wagmüllerstraße 18
Telefon: +49 89 21 26 72-0
E-Mail: poststelle@datenschutz-bayern.de
https://www.datenschutz-bayern.de

Bearbeiterin:

Dr. Verena Guttenberg

Version 1.0 | Stand: 25. April 2023

Diese Orientierungshilfe wird ausschließlich in elektronischer Form bereitgestellt. Sie kann im Internet auf https://www.datenschutz-bayern.de in der Rubrik „Datenschutzreform 2018“ abgerufen werden.

Die PDF-Datei ist für den doppelseitigen Ausdruck optimiert.

Vorwort

Viele Leistungen und Produkte, die bayerische öffentliche Stellen beschaffen, haben Bezüge zum Datenschutz. Das liegt bei Fachverfahren, mit denen personenbezogene Register geführt werden, oder bei Cloud-Lösungen, mit welchen Bürgerdaten gehostet werden sollen, auf der Hand; doch können auch Textverarbeitungsprogramme, sogar neue Aktenschränke für immer noch geführte Papierakten mehr oder weniger passgenau datenschutzrechtlichen Anforderungen und ergänzenden technisch-organisatorischen Standards entsprechen.

Die Weichen zum rechten, also (auch) datenschutzgerechten Produkt werden (spätestens) im Zuge des Beschaffungsprozesses gestellt. Bayerische öffentliche Stellen sollten die Lage dieser Weichen kennen und wissen, wie man sie zielführend bedient. Jede Beschaffung einer Leistung oder eines Produkts, das anschließend nicht rechtskonform eingesetzt werden kann, vergeudet öffentliche Mittel – und die sind bekanntlich nicht nur knapp, sondern auch von Gesetzes wegen sparsam und wirtschaftlich zu verwenden.

Die vorliegende Orientierungshilfe möchte zeigen, wie das Ziel „Datenschutzkonformität" in Beschaffungsvorgängen zur Geltung gebracht werden kann. Sie steht an der Schnittstelle von Vergaberecht und Datenschutzrecht. Die Orientierungshilfe führt durch den Ablauf des Beschaffungsprozesses, identifiziert vergaberechtliche „Einfallstore" für datenschutzrechtliche Vorgaben und erläutert, wie diese zielführend einbezogen und umgesetzt werden können. Die Handlungsmöglichkeiten eines Auftraggebers erweisen sich dabei als durchaus vielfältig.

Das von der Orientierungshilfe behandelte Thema hat jüngst auch in der Spruchpraxis der Vergabekammern sowie vereinzelt in der Rechtsprechung Aufmerksamkeit gefunden; eine systematische Aufarbeitung fehlt aber noch. Diese Lücke möchte die Orientierungshilfe schließen; aus diesem Grunde ist sie auch mit zahlreichen Nachweisen zur weiterführenden Lektüre versehen.

Die Überschneidungsbereiche von Vergaberecht und Datenschutzrecht sind bislang nicht bis ins Detail kartiert; vor diesem Hintergrund kann die Orientierungshilfe letztlich nur eine Momentaufnahme bieten. Vorschläge zu Ausbau und Verbesserung sind daher besonders willkommen und erreichen den Bayerischen Landesbeauftragten für den Datenschutz unter der Adresse **orientierungshilfen@datenschutz-bayern.de**.

Inhaltsverzeichnis

I. Einführung

Auch der öffentliche Sektor setzt zunehmend auf digitale Infrastruktur und Technologien, ob im Rahmen von E-Government-Projekten wie unter anderem der Umsetzung des Onlinezugangsgesetzes 2.0[1] oder beispielsweise beim Einsatz von Künstlicher Intelligenz. Vergabeverfahren für entsprechende Dienstleistungen oder IT-Anwendungen, die die Verarbeitung und/oder den Transfer von personenbezogenen Daten zum Gegenstand haben und somit die Vorgaben des Datenschutzrechts, insbesondere der Datenschutz-Grundverordnung berücksichtigen müssen, bergen allerdings (nicht nur) für öffentliche Auftraggeber vielfältige Herausforderungen und Fallstricke. 1

Erst im Sommer 2022 hat sich die Vergabekammer Baden-Württemberg in einer viel diskutierten Entscheidung[2] mit den Rechtmäßigkeitsvoraussetzungen einer Vergabe von Cloud-Dienstleistungen befasst und im Ergebnis potentielle Zugriffsmöglichkeiten aus dem Ausland als eine nach der Datenschutz-Grundverordnung (DSGVO) unzulässige Datenübermittlung eingestuft. 2

Das Oberlandesgericht Karlsruhe hat den Beschluss in der Beschwerdeinstanz zwar aus formal-juristischen Gründen aufgehoben.[3] Die Reaktionen auf die Entscheidungen zeigen aber ebenso wie die Spruchpraxis der Gerichte und Vergabekammern zu vergleichbaren Sachverhalten[4] deutlich, dass hinsichtlich der Anforderungen an die Beschaffung datenschutzkonformer Leistungen Unsicherheit besteht. 3

Teilweise wird daher vergaberechtswidrig ganz auf eine Beschaffung im Wettbewerb verzichtet und ohne weitere Marktbeteiligung auf bereits bekannte Vertragspartner zurückgegriffen. Dies stellt nicht nur einen Verstoß gegen § 97 Abs. 1 und 2 Gesetz gegen Wettbewerbsbeschränkungen (GWB) dar, wonach Aufträge und Konzessionen der öffentlichen Hand unter Wahrung der Grundsätze der Wirtschaftlichkeit, Verhältnismäßigkeit und Gleichbehandlung im Wettbewerb und im Wege transparenter Verfahren vergeben werden müssen,[5] sondern verkennt auch das Potential von Vergabeverfahren: So bietet das Vergaberecht zahlreiche Ansatzpunkte und Gestaltungsmöglichkeiten für die Vorgabe von datenschutzrechtlichen Anforderungen an die nachgefragte Leistung. 4

1 Entwurf eines Gesetzes zur Änderung des Onlinezugangsgesetzes sowie weiterer Vorschriften (OZG-Änderungsgesetz, Referentenentwurf des Bundesministeriums des Innern und für Heimat, Bearbeitungsstand: 20. Januar 2023, Internet: https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/aenderung-onlinezugangsgesetz.html).

2 Beschluss vom 13. Juli 2022, 1 VK 23/22, BeckRS 2022, 18405.

3 Beschluss vom 7. September 2022, 15 Verg 8/22, BeckRS 2022, 22588.

4 Vgl. nur BKartA, Beschluss vom 13. Februar 2023, VK 2-114/2, BeckRS 2023, 2260.

5 Ausnahmen hiervon gelten nur in ausdrücklich gesetzlich geregelten Fällen und insbesondere für Kooperationen öffentlicher Auftraggeber, vgl. §§ 107 ff. GWB. Zu denken ist hier an sog. Inhouse-Geschäfte im Sinne des § 108 Abs. 1 GWB, interkommunale Zusammenarbeit im Sinne des § 108 Abs. 6 GWB, Forschungs- und Entwicklungskooperationen im Sinne des § 116 Abs. 1 Nr. 2 GWB sowie das Zusammenwirken von Bund und Ländern bei informationstechnischen Systemen nach Art. 91 c Grundgesetz.

5 Im Folgenden wird für diese Leistungen der Begriff der „**datenschutzrelevanten Leistungen**“ verwendet. Gemeint sind insoweit sämtliche Leistungen, das heißt Waren oder Dienstleistungen, die die Verarbeitung personenbezogener Daten zum Gegenstand haben oder mit sich bringen und für die aus diesem Grund die Vorgaben des Datenschutzrechts Anwendung finden.

6 In Betracht kommen beispielsweise Leistungen zur Sicherstellung der Informationssicherheit, Fachverfahren für Personalverwaltung Lohnbuchhaltung und Aktenmanagement, Systeme für Videoüberwachungen und Zugangskontrollen oder auch Leistungen der Aktenvernichtung.

7 **Warnhinweis**: Es ist nicht zielführend, Leistungen zu beschaffen, die nicht rechtskonform verwendet werden können. Für Auftragnehmer ergibt sich die Pflicht zur Rechtskonformität explizit aus § 128 Abs. 1 GWB („Unternehmen haben bei der Ausführung des öffentlichen Auftrags alle für sie geltenden rechtlichen Verpflichtungen einzuhalten …“). Die öffentliche Hand als Auftraggeber im Vergaberecht unterliegt qua Rechtsnatur nach Art. 20 Abs. 3 Grundgesetz der Bindung an Recht und Gesetz und ist auch im Erst-Recht-Schluss zu § 128 Abs. 1 GWB verpflichtet, nur rechtskonform nutzbare Leistungen auszuschreiben.

8 Die Orientierungshilfe erläutert für die einzelnen Schritte von Vergabeverfahren systematisch, welche „Einfallstore“ offen stehen, wenn öffentliche Auftraggeber Waren oder Dienstleistungen beschaffen möchten, die auch den Anforderungen des Datenschutzrechts, insbesondere der Datenschutz-Grundverordnung genügen.

9 Zu differenzieren sind datenschutzrechtliche Vorgaben für die Durchführung von Vergabeverfahren als solchen. So werden insbesondere im Zusammenhang mit der Eignungsprüfung (§§ 122 ff. GWB sowie §§ 42, 44 ff. Vergabeverordnung – VgV) und der Angebotsbewertung (§ 127 GWB sowie § 58 VgV) regelmäßig personenbezogene Daten verarbeitet. Als Rechtsgrundlagen hierfür kommen für die Vergabestelle unter anderem Art. 6 Abs. 1 UAbs. 1 Buchst. c DSGVO (Erfüllung einer rechtlichen Verpflichtung) oder Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO (Erfüllung einer Aufgabe im öffentlichen Interesse) in Betracht. Bewerber und Bieter können sich bei Übermittlung personenbezogener Daten ihrer Beschäftigten gegebenenfalls zusätzlich auf eine Einwilligung nach Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO berufen;[6] in Bezug auf personenbezogene Daten von Referenzgebern kommt unter Umständen auch Art. 6 Abs. 1 UAbs. 1 Buchst. f DSGVO (Wahrung berechtigter Interessen) in Betracht. Generell haben alle Verfahrensbeteiligten insbesondere den Grundsatz der Datensparsamkeit zu beachten, den Informationspflichten nach Art. 13 und 14 DSGVO[7] nachzukommen sowie die Sicherheit der verarbeiteten personenbezogenen Daten zu gewährleisten (Art. 32 in

[6] Etwas anderes muss für Führungszeugnisse gelten. Aufgrund der hohen Sensibilität von Strafdaten ist die Vorlage von Führungszeugnissen gemäß Art. 10 Satz 1 DSGVO nur unter besonderen Voraussetzungen zulässig.

[7] Ein Muster hierfür findet sich beispielsweise in Formblatt L 2440 des vom Bayerischen Staatsministerium für Wohnen, Bau und Verkehr herausgegebenen Handbuchs für die Vergabe und Durchführung von Lieferungen und Leistungen durch Behörden der Staatsbauverwaltung des Freistaates Bayern (VHL Bayern), Ausgabe 10/2018, Internet https://www.stmb.bayern.de/buw/bauthemen/vergabeundvertragswesen/lieferunddienstleistungsauftraege/index.php.

Verbindung mit Art. 5 Abs. 1 Buchst. f DSGVO). Diese die datenschutzkonforme Durchführung von Vergabeverfahren betreffenden Aspekte bleiben im Folgenden außer Betracht.

Hinweis: Die folgenden Ausführungen gelten grundsätzlich für alle Vergaben von Waren und Dienstleistungen, sowohl oberhalb als auch unterhalb der einschlägigen Schwellenwerte für die Anwendung von EU-Vorschriften.[8] Im Interesse der besseren Lesbarkeit werden im Folgenden primär die Bestimmungen für unionsweite Vergaben in GWB und VgV referenziert. Für nationale Vergaben finden sich jeweils Entsprechungen in der Verfahrensordnung für die Vergabe öffentlicher Liefer- und Dienstleistungsaufträge unterhalb der EU-Schwellenwerte (Unterschwellenvergabeordnung – UVgO). 10

[8] Die Schwellenwerte für unionsweite Vergabeverfahren werden alle zwei Jahre von der Europäischen Union überprüft und im Regelfall auch angepasst. Der jeweilige Schwellenwert für Liefer- und Dienstleistungen ergibt sich aus Art. 4 Richtlinie 2014/24/EU in der jeweils geltenden Fassung und wird im Amtsblatt der EU bekannt gegeben. Seit 1. Januar 2022 liegt der EU-Schwellenwert für Liefer- und Dienstleistungsaufträge bei 214.000,– EUR netto.

II. Erstellung der Vergabeunterlagen

11 Das Transparenzgebot des § 97 Abs. 1 GWB verpflichtet öffentliche Auftraggeber dazu, das Beschaffungsverfahren offen und nachvollziehbar zu gestalten. Der Auftraggeber muss sich die Anforderungen an die zu vergebende Leistung und damit auch sämtliche datenschutzrechtliche Rahmenbedingungen bereits vor Einleitung des Beschaffungsvorgangs vergegenwärtigen, um sie im Vergabeverfahren umsetzen zu können. Die Vorbereitung eines Vergabeverfahrens beginnt daher mit der Bestimmung des Beschaffungsbedarfs und einer Markterkundung, § 28 VgV. Auf dieser Grundlage sind die Vergabeunterlagen nach § 29 VgV zu erstellen. Diese umfassen neben dem Anschreiben und den Bewerbungsbedingungen (§ 29 Abs. 1 Satz 2 Nrn. 1 und 2 VgV) gemäß § 29 Abs. 1 Satz 2 Nr. 3 VgV insbesondere die Vertragsunterlagen, welche wiederum aus der Leistungsbeschreibung und den Vertragsbedingungen bestehen. Nach § 29 Abs. 1 Satz 1 VgV müssen die Vergabeunterlagen alle Angaben enthalten, die erforderlich sind, um dem Bewerber oder Bieter eine Entscheidung zur Teilnahme am Vergabeverfahren zu ermöglichen.

1. Leistungsbeschreibung

12 Wesentlicher Bestandteil der Vergabeunterlagen ist zunächst die Leistungsbeschreibung, das heißt, die Beschreibung der Merkmale des Auftragsgegenstands. Diese muss gemäß § 121 Abs. 1 Satz 1 GWB **„so eindeutig und erschöpfend wie möglich“** sein, so dass die Beschreibung für alle Interessenten im gleichen Sinne verständlich ist und die Angebote miteinander verglichen werden können. § 121 Abs. 1 Satz 2 GWB in Verbindung mit § 31 VgV konkretisiert in Umsetzung von Art. 42 Abs. 2 Richtlinie 2014/24/EU[9] diese Anforderung dahingehend, dass Leistungs- oder Funktionsanforderungen oder eine Beschreibung der zu lösenden Aufgabe sowie die Umstände und Bedingungen der Leistungserbringung in verständlicher, widerspruchsfreier und nicht diskriminierender Weise festzulegen sind.

13 Nur eingeschränkt gilt dieser Bestimmtheitsgrundsatz im Zusammenhang mit sog. **funktionalen Leistungsbeschreibungen**. Diese sind dadurch gekennzeichnet, dass nur der Zweck der Leistung und die zu erreichenden Ziele verbindlich vorgegeben sind, die konkrete Art und Weise der Leistungserbringung dagegen von den Bietern eigenständig zu beschreiben ist.[10] Aber auch bei funktionalen Leistungsbeschreibungen sind die Anforderungen des Auftraggebers so spezifisch wie für den konkreten Leistungsgegenstand möglich festzulegen.

14 Ungenauigkeiten und eine nicht hinreichend eindeutige Beschreibung der gewünschten Leistung führen regelmäßig nicht nur zu einer Vielzahl von Bieterfragen, welche das Vergabe-

[9] Richtlinie 2014/24/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 über die öffentliche Auftragsvergabe und zur Aufhebung der Richtlinie 2004/18/EG (ABl. L 94 vom 28. März 2014, S. 65).

[10] Kling, in: Immenga/Mestmäcker, Wettbewerbsrecht, 6. Aufl. 2021, § 121 GWB Rn. 17; Lampert, in: Burgi/Dreher/Opitz, Beck'scher Vergaberechtskommentar, 4. Aufl. 2022, § 121 GWB Rn. 104 ff.

verfahren verzögern können. Vielmehr drohen in einem solchen Fall auch Rügen und Nachprüfungsanträge durch die Bieter, welche wiederum im äußersten Fall das Verstreichen von Fristen und das Scheitern ganzer Projekte nach sich ziehen. Schließlich kann eine ungenaue oder unvollständige Leistungsbeschreibung auch zu Schwierigkeiten bei der Vertragsumsetzung führen.

Generell kommt dem Auftraggeber bei der Ausübung seines **Leistungsbestimmungsrechts** zwar ein weiter Beurteilungsspielraum zu, der von den Nachprüfungsinstanzen nur eingeschränkt überprüfbar ist. Allerdings unterliegt das Leistungsbestimmungsrecht vergaberechtlichen Grenzen im Hinblick auf das Diskriminierungsverbot und die unionsrechtlichen Grundfreiheiten. Eine wichtige Einschränkung ergibt sich in diesem Zusammenhang aus § 31 Abs. 6 VgV, der den Auftraggeber grundsätzlich zu einer produktneutralen Leistungsbeschreibung verpflichtet. Unzulässig sind danach nicht nur ausdrückliche Produkt-, Herkunfts-, Verfahrensvorgaben oder Typenbezeichnungen, sondern auch indirekte Produktverweise, bei denen nur ein einziges bestimmtes Produkt der Leistungsbeschreibung gerecht werden kann.[11] Ausnahmen hiervon regeln § 31 Abs. 6 Satz 1 a. E. VgV (Rechtfertigung durch den Auftragsgegenstand)[12] und § 31 Abs. 6 Satz 2 VgV (Auftragsgegenstand nicht hinreichend genau und allgemein verständlich beschreibbar).[13] In letzterem Fall muss allerdings durch den Zusatz „oder gleichwertig“ eine sog. Gleichwertigkeitsklausel in die Beschreibung mit aufgenommen werden, und der Auftraggeber muss festlegen, welche Anforderungen er an die Gleichwertigkeit stellt. Darüber hinaus hat der Auftraggeber bei der Ausübung seines Leistungsbestimmungsrechts das Gebot der Losaufteilung nach § 97 Abs. 4 GWB zu beachten.[14] 15

[11] Schellenberg, in: Pünder/Schellenberg, Vergaberecht, 3. Aufl. 2019, § 31 VgV Rn. 80.

[12] Der Auftraggeber muss hierfür ein legitimes Interesse aufgrund objektiver, sach- und auftragsbezogener Gründe geltend machen (Willkürmaßstab), Lampert, in: Burgi/Dreher/Opitz, Beck'scher Vergaberechtskommentar, 3. Aufl. 2019, § 31 VgV Rn. 98; Siebler/Hamm, Produktfestlegungen in Vergabeverfahren - Zulässigkeit und Grenzen unter Berücksichtigung der Entwicklung in der aktuellen Rechtsprechung, ZfBR 2022, 240, 243 m. w. N. In der Rechtsprechung anerkannt wurden beispielsweise ein Risiko von Fehlfunktionen, Kompatibilitätsproblemen und höherer Zeit-und Kostenaufwand für Schulungen (OLG Düsseldorf, Beschluss vom 13. April 2016, Verg 47/15, BeckRS 2016, 13046, zum inhaltlich vergleichbaren § 8 EG Abs. 7 VOL/A); das Bedürfnis, Versicherte mit vertrauten Produkten zu versorgen (BKartA, Beschluss vom 17. April 2014, VK 1-22/14, BeckRS 2014, 121406, ebenfalls zum inhaltlich vergleichbaren § 8 EG Abs. 7 VOL/A); die Erforderlichkeit einer bestimmten Schnittstelle für eine App (BayObLG München, Beschluss vom 29. Juli 2022, Verg 13.21, BeckRS 2022, 19230). Dagegen wurden Schnittstellenprobleme und Wirtschaftlichkeitsverluste nicht für ausreichend erachtet (VK Lüneburg, Beschluss vom 12. Mai 2005, VgK-15/2005, BeckRS 2005, 06303, zu § 8 Nr. 3 Abs. 5 VOL/A).

[13] Lampert, in: Burgi/Dreher/Opitz, Beck'scher Vergaberechtskommentar, 3. Aufl. 2019, § 31 VgV Rn. 113. Der Auftraggeber darf auch nicht bestimmte Produkte lediglich beispielhaft benennen und mit dem Zusatz „oder gleichwertig“ bzw. „oder gleichwertiger Art“ versehen, da die Wettbewerber für alle Spezifika des Leitprodukts die Gleichwertigkeit nachweisen müssten, was wiederum eine Wettbewerbsverzerrung darstellt, Schellenberg, in: Pünder/Schellenberg, Vergaberecht, 3. Aufl. 2019, § 31 VgV Rn. 82 m.w.N. – A. A. OLG Düsseldorf, Beschluss vom 9. Januar 2013, VII-Verg 33/12, BeckRS 2013, 4078, das eine „unechte Produktorientierung“ grundsätzlich für zulässig hält.

[14] Gemäß § 97 Abs. 4 GWB sind bei der Vergabe öffentlicher Aufträge mittelständische Interessen zu berücksichtigen und Leistungen in der Menge aufgeteilt (Teillose) und getrennt nach Art oder Fachgebiet (Fachlose) zu vergeben, es sei denn, wirtschaftliche oder technische Gründe erfordern eine gemeinsame Vergabe. Konkretisierende Vorgaben finden sich insoweit in § 30 VgV.

II. Erstellung der Vergabeunterlagen

16 Konkret bezogen auf datenschutzrelevante Leistungen bedeutet dies, dass die Vorgaben betreffend Datenschutz und Datensicherheit schon in der Leistungsbeschreibung eindeutig und erschöpfend niederzulegen sind beziehungsweise in Rahmenbedingungen einer funktionalen Leistungsbeschreibung festgelegt werden müssen. Öffentliche Auftraggeber sind im Rahmen ihrer Gesetzesbindung verpflichtet, Datenschutzrecht, insbesondere die Datenschutz-Grundverordnung zu beachten. Mit Leistungen, die diesen Anforderungen in ihren Ausprägungen für die jeweilige öffentliche Stelle nicht voll entsprechen, kann diese letztlich „nichts anfangen".

17 Das bedeutet: Werden im Zusammenhang mit der jeweiligen Leistung personenbezogene Daten (z. B. Bürgerdaten) verarbeitet, muss der Auftraggeber als datenschutzrechtlich Verantwortlicher nach Art. 5 Abs. 2 DSGVO schon durch die Beschreibung der Leistung sicherstellen, dass die jeweilige Verarbeitung rechtskonform erfolgt, das heißt sämtliche **zwingenden Vorgaben der Datenschutz-Grundverordnung** erfüllt. Insbesondere muss die Verarbeitung über einen der Erlaubnistatbestände des Art. 6 DSGVO legitimiert, also rechtmäßig im Sinne des Art. 5 Abs. 1 Buchst. a DSGVO sein; auch müssen die betroffenen Personen in einer Datenschutzerklärung im Sinne des Art. 13 DSGVO über die Verarbeitung informiert werden.[15] Zudem ist bei der Gestaltung der Leistungsbeschreibung ein besonderer Fokus auf die Grundsätze der Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO) und die Sicherheit der Verarbeitung (Art. 32 in Verbindung mit Art. 5 Abs. 1 Buchst. f DSGVO) zu legen: Die Inhalte des Leistungsgegenstandes sind so zu gestalten, dass personenbezogene Daten nur verarbeitet werden, soweit dies für den jeweiligen Verarbeitungszweck erforderlich ist und entsprechende technische Anforderungen die jeweils notwendige Datensicherheit gewährleisten. Die konkreten Anforderungen hängen dabei von der Art der personenbezogenen Daten und dem jeweiligen Verarbeitungszweck ab. Daneben kann der Auftraggeber individuell noch weitere (datenschutzrechtliche) Anforderungen an die Leistung festlegen.

18 Zugleich müssen öffentliche Auftraggeber darauf achten, dass die datenschutzrechtlichen Anforderungen an den Beschaffungsgegenstand den Markt für potentielle Bieter vor dem Hintergrund des vergaberechtlichen Wettbewerbsprinzips nicht unverhältnismäßig verengen. So müssen die vom Auftraggeber festgelegten datenschutzrechtlichen Vorgaben durch den Leistungsgegenstand sachlich gerechtfertigt sein; sie dürfen nicht diskriminierend sein und müssen auf nachvollziehbaren objektiven und auftragsbezogenen Gründen basieren. Diese Aspekte sind ebenso wie eine eventuelle Beschränkung des Wettbewerbs aufgrund von (datenschutzrechtlichen) Leistungsspezifitäten (z. B. Erfordernis einer bestimmten Verschlüsselungstechnik) auf der Grundlage von § 31 Abs. 6[16] beziehungsweise § 14 Abs. 3 Nr. 2 VgV[17] im Vergabevermerk nach § 8 VgV nachvollziehbar zu dokumentieren.

[15] Die Leistungsbeschreibung kann dabei allgemeiner formuliert werden und den späteren Auftragnehmer pauschal zur Einhaltung „sämtlicher datenschutzrechtlicher Anforderungen" verpflichten. Der Auftraggeber kann die einzelnen Pflichten aber auch detailliert vorschreiben. Maßstab muss stets die Rechenschaftspflicht des Auftraggebers als Verantwortlichen sein.

[16] S. o. Rn. 15.

[17] Nach § 14 Abs. 4 Nr. 2 VgV kann der öffentliche Auftraggeber Aufträge im Verhandlungsverfahren ohne Teilnahmewettbewerb vergeben, wenn zum Zeitpunkt der Aufforderung zur Abgabe von Angeboten der Auftrag nur von einem bestimmten Unternehmen erbracht oder bereitgestellt werden kann, weil (Buchst. a) ein einzigartiges Kunstwerk oder eine einzigartige künstlerische Leistung erschaffen oder erworben werden soll, oder

a) Bestimmung des Beschaffungsbedarfs

In Vorbereitung der Erstellung der Leistungsbeschreibung ist mithin zunächst der Beschaffungsbedarf, das heißt der Gegenstand der Leistung, zu bestimmen. Dem sollten eine **Markterkundung** in Gestalt einer Situationsanalyse über die anbietenden Unternehmen, die vorhandenen Produkte, den Technologiestand, die rechtlichen und zeitlichen Rahmenbedingungen und die möglichen finanziellen Aufwendungen sowie eine Analyse der Risiken für die Rechte und Freiheiten betroffener Personen zugrunde liegen.[18] Das Ergebnis dieser Überprüfung muss anschließend in verständlich formulierte und widerspruchsfreie Anforderungen an die zu beschaffende Leistung umgesetzt werden. In der Regel arbeitet die Vergabestelle des öffentlichen Auftraggebers insoweit eng mit der Bedarfsstelle, das heißt den betroffenen Fachbereichen und insbesondere der IT, zusammen. 19

Praxishinweis: Bereits in dieser Phase sollten bayerische öffentliche Stellen ihre behördlichen Datenschutzbeauftragten (und gegebenenfalls Informationssicherheitsbeauftragten) einbinden. Die Möglichkeit, datenschutzrechtliche Anforderungen frühzeitig zu benennen und in Anforderungen an die zu beschaffende Leistung zu konkretisieren, sollten behördliche Datenschutzbeauftragte konsequent nutzen. Öffentliche Stellen, die externe Datenschutzbeauftragte beauftragen möchten, sollten darauf achten, dass entsprechende Leistungen von dem gebuchten „Paket" umfasst sind und auch in der nötigen Quantität und Qualität abgerufen werden können. 20

Gegenstand der **Risikoanalyse** ist bei der Beschaffung von datenschutzrelevanten Leistungen die Frage, welche Risiken und (materiellen oder immateriellen) Folgen für die Rechte von betroffenen Personen bei Risikoeintritt aus der leistungsgegenständlichen Verarbeitung und gegebenenfalls dem Transfer von Daten resultieren können (auch: Datenschutz-Sicherheitskonzept).[19] Je nach der zu bewertenden Verarbeitung kann eine allgemeine Risikoanalyse ausreichen oder bei Hochrisikoverarbeitungen eine Datenschutz-Folgenabschätzung im Sinne des Art. 35 DSGVO[20] erforderlich sein. Dabei gilt: Je sensibler die Daten, desto höher das Risiko für die betroffenen Personen und umso höher die Anforderungen an den Schutz dieser Daten. Dies entspricht auch dem risikobasierten Ansatz der Datenschutz-Grundverordnung. Als weitere Kriterien sind unter anderem die Kategorien personenbezogener Daten[21], die Anzahl der von der Verarbeitung betroffenen Personen, die Datenmenge, die Häufigkeit von Transfers sowie die Eintrittswahrscheinlichkeit eines Risikos und der potentielle 21

– für datenschutzrechtliche Anforderungen deutlich praxisrelevanter – weil (Buchst. b) aus technischen Gründen kein Wettbewerb vorhanden ist oder (Buchst. c) wegen des Schutzes von ausschließlichen Rechten, insbesondere von gewerblichen Schutzrechten.

18 Fehlen ausreichende Erkenntnismöglichkeiten, können diese Prüfungsschritte ausnahmsweise auch in ein laufendes Ausschreibungsverfahren implementiert werden. Insoweit ist allerdings ein besonderer Aufwand zur Herstellung von Transparenz für alle Verfahrensbeteiligten erforderlich.

19 Zum Ganzen Bayerischer Landesbeauftragter für den Datenschutz, Risikoanalyse und Datenschutz-Folgenabschätzung, Orientierungshilfe, Stand 5/2022, Internet: https://www.datenschutz-bayern.de, Rubrik „DSFA".

20 Ausführlich hierzu Bayerischer Landesbeauftragter für den Datenschutz, Datenschutz-Folgenabschätzung, Orientierungshilfe, Stand 2/2021, Internet: https://www.datenschutz-bayern.de, Rubrik „DSFA".

21 Bei besonderen Kategorien personenbezogener Daten gelten gegebenenfalls spezifische Verarbeitungsanforderungen, vgl. nur Art. 9 DSGVO und § 80 Abs. 2 Zehntes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz –.

Schaden zu berücksichtigen. In diesem Zusammenhang spielen insbesondere der Ort der Datenverarbeitung und die Bewertung technischer und organisatorischer Schutzmaßnahmen eine Rolle. Zu prüfen ist, ob der Ort der Datenverarbeitung Auswirkungen auf die Eignung und Nutzbarkeit der Leistung, auf den Datenschutz und die IT-Sicherheit sowie auf die Kosten hat, und ob ein gegebenenfalls erforderlicher Datentransfer nach Art. 44 ff. DSGVO zulässig ist.[22] Für die Bewertung technischer Schutzmaßnahmen sind die Möglichkeiten von Verschlüsselung, Anonymisierung und Pseudonymisierung sowie das Vorhandensein anerkannter Zertifikate maßgeblich. Nach Art. 24 Abs. 1 Satz 1, Art. 32 Abs. 1 DSGVO ist jeder Verantwortliche verpflichtet, mittels der wirksamen Umsetzung von technischen und organisatorischen Maßnahmen ein dem Verarbeitungsrisiko angemessenes Schutzniveau zu gewährleisten.[23]

22 Auf dieser Grundlage ist der Beschaffungsbedarf zu bestimmen und zu beschreiben. Dazu gehören zum einen die **funktionalen und technischen Anforderungen** an den Leistungsgegenstand. Je nach Einzelfall muss der Auftraggeber bei der Ausschreibung von datenschutzrelevanten Leistungen Angaben zu Hardware, Software, Lizenzen, Spezifikationen, Tests, Dokumentationen, Handbüchern und Schulungen machen, gegebenenfalls verknüpft mit zeitlichen Vorgaben und/oder inhaltlichen Meilensteinen (das heißt überprüfbaren Zwischenzielen). Zudem hat der Auftraggeber die räumlichen und physikalischen Umgebungsanforderungen, die Sicherheitsanforderungen, notwendige Mitwirkungsleistungen des Auftraggebers und – sofern relevant – die bereits vorhandene IT-Infrastruktur sowie auftraggeberseitige Leit- und Richtlinien zu beschreiben. Soweit möglich, sollten schließlich auch Algorithmen, Datenstrukturen, Datenformate und Schnittstellen einfließen. Wichtige Orientierungshilfe bieten insofern die „Ergänzenden Vertragsbedingungen für die Beschaffung von IT-Leistungen“ (**EVB-IT**)[24] sowie die „Unterlage für Ausschreibung und Bewertung von IT-Leistungen“ (**UfAB 2018**).[25] Dabei ist stets zu beachten, dass die Festlegung auf bestimmte Lösungen den Wettbewerb nicht unrechtmäßig einschränkt und die zentralen Werte des § 97 GWB nicht ausgehöhlt werden.

[22] Näher Bayerischer Landesbeauftragter für den Datenschutz, Office-Anwendungen aus Drittstaaten bei bayerischen öffentlichen Stellen, Aktuelle Kurz-Information 39, Stand 12/2021, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018“.

[23] Zur Überführung der Anforderungen der Grundsätze des Art. 5 DSGVO in entsprechende Gewährleistungsziele und technische und organisatorische Maßnahmen vgl. das von der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) gebilligte sog. Standard-Datenschutzmodell, Internet: https://www.datenschutz-mv.de/datenschutz/datenschutzmodell.

[24] Die Musterverträge decken nahezu das gesamte Anwendungsspektrum der IT-Beschaffung ab und setzen gemeinsame Standards. Sie werden von der Arbeitsgruppe EVB-IT, die vom Bundesministerium des Innern und für Heimat geleitet wird, mit der IT-Wirtschaft, vertreten durch den Bitkom e. V., verhandelt und auf der Homepage des Beauftragten der Bundesregierung für Informationstechnik (https://www.cio.bund.de) kostenfrei zur Verfügung gestellt.

[25] Die vom Beschaffungsamt des Bundesministeriums des Innern und für Heimat herausgegebene Unterlage ist nicht verbindlich. Sie gibt in Gestalt eines Praxisleitfadens für die Durchführung von IT-Beschaffungen unter anderem Hinweise und Empfehlungen zur Vorbereitung von Vergabeverfahren, Empfehlungen zur Ermittlung des wirtschaftlichsten Angebots und zur Anwendung bestimmter Bewertungsmethoden. Dieser ist ebenfalls auf der Homepage des Beauftragten der Bundesregierung für Informationstechnik kostenfrei abrufbar.

Bei der Beschreibung der Leistung können gemäß § 31 Abs. 3 Satz 1 VgV zusätzlich auch **innovative, soziale und umweltbezogene Aspekte** berücksichtigt werden. Für datenschutzrelevante Leistungen, die zumeist dem Bereich der Informations- und Kommunikationstechnik zuzuordnen sind, kommen dabei insbesondere innovative Leistungsmerkmale wie die Organisation von Softwareimplementierungs- und -wartungsverträgen[26], innovative Lösungen im Rahmen funktionaler Ausschreibungen von IT-Leistungen[27] oder der innovative Einsatz von Künstlicher Intelligenz in Betracht. 23

Rein formal sind nach § 121 Abs. 2 GWB bei der Erstellung der Leistungsbeschreibung für Leistungen, die zur Nutzung durch natürliche Personen vorgesehen sind, außer in ordnungsgemäß begründeten Fällen die **Zugänglichkeitskriterien** für Menschen mit Behinderungen oder die Konzeption für alle Nutzer zu berücksichtigen. 24

b) Leistungsort

Im Rahmen der Leistungsbeschreibung sollte auch der Leistungsort bestimmt werden. Dieser ist als Teil des Lebenszyklus beziehungsweise der Produktionskette eines Auftrags im Sinne des § 31 Abs. 3 Satz 2 VgV[28] für datenverarbeitende Projekte mit Blick auf die Vorgaben der Datenschutz-Grundverordnung und die Rechtsprechung des Europäischen Gerichtshofs, insbesondere in der Rechtssache „Schrems II“,[29] von besonderer Relevanz. 25

Personenbezogene Daten dürfen nur dann in ein Land außerhalb der EU beziehungsweise des Europäischen Wirtschaftsraums (sog. Drittland) übermittelt werden, wenn einer der besonderen Erlaubnisgründe der Art. 44 ff. DSGVO vorliegt. Zulässig ist eine Datenübermittlung in ein Drittland hiernach insbesondere dann, wenn die Kommission in einem Beschluss das angemessene Schutzniveau des Drittlands festgestellt hat (sog. Angemessenheitsbeschluss, vgl. Art. 45 Abs. 1 DSGVO). Für die USA, deren Unternehmen den Markt im Bereich Software und IT-Ausstattung weithin dominieren, liegt ein solcher Beschluss ausdrücklich nicht vor; vielmehr hat der Europäische Gerichtshof mit Urteil vom 16. Juli 2020 (C-311/18 „Schrems II“) die Datenschutzvereinbarung der Europäischen Union mit den USA („Privacy Shield“) für ungültig erklärt. Das Datenschutzniveau in den USA entspricht laut Europäischem Gerichtshof nicht den Standards des europäischen Datenschutzes und verstößt gegen Art. 7, 8 und 47 Charta der Grundrechte der Europäischen Union, denn die Befugnisse der US-Behörden – insbesondere die Überwachungsprogramme und Zugriffsbefugnisse auf Grundlage von 50 U.S.C. § 1881a beziehungsweise Sec. 207 des Foreign Intelligence Surveillance Act (FISA 702), der Executive Order 12333 und der Presidential Policy Directive 28 – erlauben es, auf personenbezogene Daten der EU-Bürger heimlich und ohne effektive Rechtsbehelfsmöglichkeiten zuzugreifen, und sind zudem unverhältnismäßig. Im März 2022 einigten sich die USA und die EU dem Grunde nach auf ein Nachfolgeabkommen, in dem die Bedenken des 26

[26] OLG Karlsruhe, Beschluss vom 5. November 2014, 15 Verg 6/14, BeckRS 2015, 4323.

[27] BKartA, Beschluss vom 14. Oktober 2013, VK 2-84/13, IBRRS 2013, 4843.

[28] Rosenkötter/Hansen/Tegeler, Berücksichtigung datenschutzrechtlicher Aspekte in Vergabeverfahren nach „Schrems II“, NZBau 2021, 355, 360.

[29] EuGH, Urteil vom 16. Juli 2020, C-311/18.

Europäischen Gerichtshofs berücksichtigt worden sein sollen. Dieses wird jedoch frühestens Mitte 2023 in Kraft treten[30] und wird von Datenschützern bereits jetzt kritisiert.

27 Liegt kein wirksamer Angemessenheitsbeschluss vor, ist eine Datenübermittlung vorbehaltlich geeigneter Garantien gemäß Art. 46 Abs. 1 DSGVO in Betracht zu ziehen. Diese Garantien können insbesondere gemäß Art. 46 Abs. 2 Buchst. c DSGVO in sogenannten Standarddatenschutzklauseln bestehen. Ein entsprechendes aktuelles Klauselwerk hat die Europäische Kommission im Sommer 2021 bereitgestellt.[31] Dieses muss aber tatsächlich wirksam sein. Dazu bedarf es einer Risikobewertung der geplanten Datenübermittlung auf der Grundlage einer Betrachtung der Heimatrechtsordnung des ausländischen Datenempfängers („Transfer Impact Assessment"). Der Europäische Datenschutzausschuss hat für diese Betrachtung ausführliche Hinweise veröffentlicht.[32] Soweit Datenübermittlungen in die USA in Rede stehen, sind für die Wirksamkeit des vereinbarten Klauselwerks wiederum die Vorgaben der „Schrems II"-Entscheidung des Europäischen Gerichtshofs zu beachten. Danach ist die tatsächliche Wirksamkeit des vereinbarten Klauselwerks dann anzunehmen, wenn der Verantwortliche den Nachweis erbringt, dass die zu übermittelnden personenbezogenen Daten aus Rechtsgründen von vornherein nicht Gegenstand von Zugriffsrechten US-amerikanischer Behörden werden können. Lässt sich dieser Nachweis nicht führen, ist als Kompensation eine Verschlüsselung und/oder Pseudonymisierung der personenbezogenen Daten in Betracht zu ziehen. Der Verantwortliche muss in diesem Fall zudem den Nachweis erbringen, dass eine Aufhebung der Verschlüsselung und/oder Pseudonymisierung bei dem ausländischen Vertragspartner durch Behörden seines Heimatstaats ausgeschlossen werden kann. Welche Kompensationsmaßnahmen im Einzelnen notwendig und ausreichend sind, ist grundsätzlich aus technisch-organisatorischer Sicht zu bewerten. Für Datentransfers in die USA bedeutet das, dass die Standardvertragsklauseln für sich genommen keine solchen

[30] Am 7. Oktober 2022 hat der US-amerikanische Präsident Biden die Executive Order On Enhacing Safeguards for United States Signals Intelligence Activities verabschiedet, um das EU-U.S. Data Privacy Framework als Nachfolger des Privacy Shield Framework umzusetzen, Internet: https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities. Die EU-Kommission hat auf dieser Grundlage ein Verfahren für die Bewertung in einem Angemessenheitsbeschluss eingeleitet. Dieser liegt seit dem 13. Dezember 2022 als Entwurf vor, vgl. Adequacy decision for the EU-US Data Privacy Framework, Internet: https://commission.europa.eu/document/e5a39b3c-6e7c-4c89-9dc7-016d719e3d12_en. Der Europäische Datenschutzausschuss hat hierzu am 28. Februar 2023 eine unverbindliche Stellungnahme abgegeben, Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework, 28 February 2023, Internet: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-52023-european-commission-draft-implementing_de. Zusätzlich muss ein Ausschuss, der sich aus Vertretern der EU-Mitgliedstaaten zusammensetzt, den Vorschlag mit qualifizierter Mehrheit billigen. Auch das EU-Parlament kann sich in einer formellen Stellungnahme äußern. Deshalb ist derzeit noch nicht absehbar, wann der neue Angemessenheitsbeschluss in Kraft treten wird.

[31] Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln („Standard Contractual Clauses", SCC) für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates (ABl. L 199 vom 7. Juni 2021, S. 31 ff.). Diese sind seit dem 27. September 2021 zwingend für Neuverträge anzuwenden; eine Umstellung von Altverträgen musste bis zum 27. Dezember 2022 erfolgen.

[32] Europäischer Datenschutzausschuss, Empfehlungen 01/2020 vom 18. Juni 2021, Rn. 28 ff., Internet: https://edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo2.0_supplementarymeasurestransfertools_de.pdf.

Transfers ermöglichen; vielmehr müssen sie einzelfallbezogen zwingend mit technischen Maßnahmen kombiniert werden, um das Datenschutzniveau als angemessen bewerten zu können.[33]

28 Gerade bei Leistungen betreffend die Verarbeitung personenbezogener Daten und insbesondere bei der Anwendung von Cloud-Lösungen (siehe Rn. 84 ff.) ist die Beschränkung des Leistungsortes auf die EU beziehungsweise den Europäischen Wirtschaftsraum (EWR) sowie auf Staaten, für die es einen Angemessenheitsbeschluss gibt, für öffentliche Auftraggeber daher dringend anzuraten[34] und in Nr. 4 EVB-IT Cloud AGB sogar explizit geregelt.[35] Dies stellt zwar eine Beschränkung des allgemeinen Grundsatzes dar, dass Auftraggeber durch Vorfestlegungen zum Beschaffungsgegenstand den Wettbewerb nicht unangemessen einschränken oder bestimmte Anbieter diskriminieren beziehungsweise bevorzugen dürfen, § 31 Abs. 1 VgV. Allerdings kann der Auftragsgegenstand gemäß § 31 Abs. 6 Satz 1 VgV a. E. ausnahmsweise Einschränkungen dieses Grundsatzes rechtfertigen, sofern diese objektiv sachlich begründet und nicht durch die Absicht der Bevorzugung eines bestimmten Unternehmens motiviert sind.[36] Für die Beschränkung des Leistungsortes ergibt sich die Rechtfertigung für öffentliche Auftraggeber aus der Verpflichtung zur Einhaltung der Datenschutz-Grundverordnung.

c) Verfügbarkeit und Dienstgüte

29 Weiterer Bestandteil der Leistungsbeschreibung sind Festlegungen des Auftraggebers zu erwarteter Verfügbarkeit und Dienstgüte. Bezogen auf datenschutzrelevante Leistungen umfasst die **Verfügbarkeit** nicht nur deren leistungsbezogene Definition, das heißt die Bestimmung, welche Daten in welchem Format mit welchen Ressourcen verarbeitet werden. Es geht insoweit auch um die Frage, wann Verfügbarkeit gegeben ist und wann Zeiten geplanter Nichtverfügbarkeit (z. B. für Wartungsarbeiten) stattfinden dürfen, wann eine Minderung der

33 EuGH, Urteil vom 16. Juli 2020, C-311/18 (Schrems II).

34 Zumindest inzident anerkannt in den Entscheidungen der VK Baden-Württemberg, Beschluss vom 13. Juli 2022, 1 VK 23/22, BeckRS 2022, 18405, und des OLG Karlsruhe, Beschluss vom 7. September 2022, 15 Verg 8/22, BeckRS 2022, 22588. In der Konstellation, dass ein potentieller Auftragnehmer für eine Auftragsverarbeitung zwar seinen Sitz in der EU bzw. dem EWR hat, aber Tochterunternehmen einer Mutter mit Sitz in einem Drittstaat ist, kann aufgrund von Normen dieses Drittstaats (insbesondere USA) die abstrakte Gefahr einer nach EU-Recht unzulässigen Übermittlung personenbezogener Daten aus der EU in einen Drittstaat begründet werden. An die gemäß Art. 28 Abs. 1, Erwägungsgrund 81 DSGVO erforderliche Prüfung der Zuverlässigkeit des Auftragsverarbeiters sind in diesem Fall nach einem Beschluss der DSK besonders hohe Anforderungen zu stellen, die dieser Gefahr Rechnung tragen (DSK, Zur datenschutzrechtlichen Bewertung von Zugriffsmöglichkeiten öffentlicher Stellen von Drittländern auf personenbezogene Daten, Beschluss vom 31. Januar 2023, Internet: https://www.datenschutzkonferenz-online.de/beschluesse-dsk.html). Sollte der Verantwortliche nach dieser Prüfung zu der Bewertung kommen, dass der Auftragsverarbeiter keine hinreichenden Garantien gemäß Art. 28 Abs. 1 DSGVO bietet, muss er selbst technische und organisatorische Maßnahmen ergreifen, um die festgestellten Defizite auszugleichen und so die Risiken einer unzulässigen Drittlandsübermittlung zu vermeiden.

35 Nach Nr. 4 EVB-IT Cloud hat die Speicherung und sonstige Verarbeitung von Daten des Auftraggebers durch den Auftragnehmer ausschließlich innerhalb der EU und des EWR zu erfolgen sowie, sofern ein Angemessenheitsbeschluss gemäß Art 45 DSGVO besteht, in der Schweiz. Eine Ausnahme greift nur dann, wenn der Auftraggeber in der Administrationskonsole zusätzlich weitere Regionen für die Leistung ausgewählt hat.

36 BayObLG München, Beschluss vom 29. Juli 2022, Verg 13.21, BeckRS 2022, 19230 m. w. N.

Verfügbarkeit[37] vorliegt sowie gegebenenfalls die Festlegung korrelierender Vertragsstrafen und die Bestimmung des Verantwortlichen für die Feststellung der Verfügbarkeit.[38] Auch Notfallszenarien und entsprechende (Abhilfe-)Maßnahmen sollten definiert werden.[39]

30 Die Anforderungen im Zusammenhang mit der **Dienstgüte** (oder auch „quality of service") sollen daneben sicherstellen, dass die Leistungen den tatsächlichen Anforderungen des öffentlichen Auftraggebers entsprechen, das heißt zuverlässig und performant erfolgen.

d) Regelungen zum Vertragsende

31 Schließlich können schon in der Leistungsbeschreibung (oder in den Vertragsbestimmungen) Regelungen zum Vertragsende getroffen werden. Diese können insbesondere Vertraulichkeitsabreden, die Bereitstellung bestimmter Informationen durch die Vertragsparteien, Löschpflichten sowie die Verpflichtung des Auftragnehmers zur Unterstützung bei der Migration an den Auftraggeber selbst oder einen Folgeauftragnehmer umfassen. Die konkrete Ausgestaltung ist abhängig vom jeweiligen Einzelfall.

e) Datenschutz/Datensicherheit

aa) Allgemeines

32 Einer der Kernpunkte der Beschreibung datenschutzrelevanter Leistungen sind jedoch die Anforderungen des öffentlichen Auftraggebers an Datenschutz und Datensicherheit. Öffentliche Auftraggeber sind als Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO auch verpflichtet, die Verpflichtungen nach Art. 24 Abs. 1 und 2 sowie Art. 32 Abs. 1 und 2 DSGVO zu erfüllen.

33 Im Rahmen der Leistungsbeschreibung sollte der Auftraggeber daher Ausführungen zu den für ein ausreichendes Datenschutzniveau erforderlichen technischen und organisatorischen Maßnahmen machen. Wichtige Anhaltspunkte hierfür können sich unter anderem aus den Mustern der EVB-IT, den Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) als Bestandteil des IT-Grundschutzes[40] sowie aus den Richtlinien und Leitfäden des Landesamts für Sicherheit in der Informationstechnik[41] ergeben.

34 Bei **organisatorischen Maßnahmen** zur Gewährleistung eines angemessenen Datenschutzniveaus ist dabei unter anderem an eindeutige Erläuterungen zu Verarbeitungsprozessen, transparenzsteigernde Maßnahmen, die Umsetzung der Grundsätze der Datenminimierung und Zweckbindung, Lösch- und Berichtigungskonzepte sowie etablierte Vorgehensweisen betreffend Informationspflichten und Auskunftsersuchen zu denken. Insoweit kommen

[37] Zu denken ist hier an eine Beschreibung der möglichen Verfügbarkeitsminderungen und -ausfälle, z. B. Systemstörungen, Löschung von Daten etc. Für den Ausschluss von Versäumnissen aus der Sphäre des öffentlichen Auftraggebers und Fälle höherer Gewalt Claßen/Koch/Müller, Beschaffung von Cloud-Services durch öffentliche Auftraggeber, MMR 2020, 723, 726.

[38] Zum Ganzen vgl. die musterhaften Regelungen in Nr. 8 EVB-IT Cloud AGB und Nr. 19 ff. EVB-IT Anlage Kriterienkatalog für Cloud-Leistungen.

[39] Zum Beispiel regelmäßige Backups und ständig erreichbare Ansprechpartner.

[40] Internet: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html.

[41] Internet: https://lsi.bybn.de/ikt/index.php (nur über das Bayerische Behördennetz abrufbar).

daher beispielsweise die Vorgabe von definierten Vorgehensmodellen für alle IT-Prozesse wie etwa nach ITIL („Information Technology Infrastructure Library“) oder COBIT („Control Objectives for Information und Related Technology“), eine nachhaltige Umsetzung eines Informationssicherheitskonzepts (z. B. in Anlehnung an ISO 27001), eine angemessene Organisationsstruktur für Informationssicherheit und die Vereinbarung vertraglicher Zusagen zur Abwehr möglicher staatlicher Zugriffsversuche in Betracht. Diese Anforderungen können allerdings nur im Verhältnis zwischen Auftraggeber und Auftragnehmer durchsetzbare Wirkung entfalten und garantieren für sich genommen kein angemessenes Datenschutzniveau der beauftragten Leistung.

Ergänzend sollten daher **technische Maßnahmen** physisch den Zugriff auf Daten verhindern. Denkbar sind insoweit – sofern im Einzelfall nach Art der Leistung möglich und erforderlich – Maßnahmen der Verschlüsselung, Pseudonymisierung und Anonymisierung. Die hierfür erforderlichen Anwendungen können ebenfalls Bestandteil des Beschaffungsgegenstands sein.[42] **35**

Zur Sicherstellung der Gewährleistung dieser Anforderungen kann der Auftraggeber in den Grenzen des § 31 Abs. 6 VgV unter Einbeziehung vergleichbarer Standards von den Bietern auch den Nachweis bestimmter **Datenschutzaudits** und/oder die Vorlage bestimmter **Zertifizierungen** für die ausgeschriebenen IT-Produkte oder Dienstleistungen verlangen.[43] Beispielhaft sind hier Zertifizierungen nach BSI IT-Grundschutz, die Zertifizierung von Informationssicherheitsmanagementsystemen nach ISO 27001 sowie datenschutzspezifische Zertifizierungsverfahren, Datenschutzsiegel und Datenschutzprüfzeichen nach Art. 42 DSGVO[44] zu nennen. Eine Zertifizierung mindert allerdings nicht die Verantwortung zur Einhaltung der Datenschutz-Grundverordnung.[45] Im Übrigen ist zu beachten, dass manche Zertifizierungen oder Audits auch dann verliehen werden können, wenn das mittels Zertifizierung oder Audit nachzuweisende Datenschutzniveau nicht vollständig erreicht wird. Der öffentliche Auftraggeber muss sich daher vor Festlegung eines bestimmten Zertifizierungs- oder Auditerfordernisses vergewissern, ob dieses tatsächlich zum Nachweis des gewünschten Datenschutzniveaus sinnvoll und tauglich ist. **36**

Betreiber Kritischer Infrastrukturen wie Strom- und Wasserversorgung, Finanzen oder Ernährung sind zum Schutz der Sicherheit und Verfügbarkeit ihrer IT-Systeme zudem auf die sog. **37**

42 Rosenkötter/Hansen/Tegeler, Berücksichtigung datenschutzrechtlicher Aspekte in Vergabeverfahren nach „Schrems II“, NZBau 2021, 355, 360.

43 Ein Datenschutzaudit bezieht sich dabei auf ein Verfahren, das eine Organisation(seinheit) verwendet, und richtet sich auf die Prüfung eines Datenschutzmanagementsystems sowie die Bestätigung, dass dieses zu einer kontinuierlichen Verbesserung des Datenschutzes beiträgt. Eine Zertifizierung ist demgegenüber auf ein bestimmtes IT-Produkt oder eine Dienstleistung gerichtet. Zu Ganzen Hornung/Hartl, Datenschutz durch Marktanreize – auch in Europa? – Stand der Diskussion zu Datenschutzzertifizierung und Datenschutzaudit, ZD 2014, 219.

44 Beachte hierzu Europäischer Datenschutzausschuss, Leitlinien 1/2018 für die Zertifizierung und Ermittlung von Zertifizierungskriterien nach den Artikeln 42 und 43 der Verordnung (EU) 2016/679, Stand 6/2019.

45 Für datenschutzspezifische Zertifizierungsverfahren, Datenschutzsiegel und Datenschutzprüfzeichen explizit geregelt in Art. 42 Abs. 4 DSGVO.

KRITIS-Regulierung (Sicherheit Kritischer Infrastrukturen) mit unter anderem dem IT-Sicherheitsgesetz 2.0[46] verpflichtet.

bb) Auftragsdatenverarbeitung, Art. 28 Abs. 3 DSGVO

38 Besondere Anforderungen an Datenschutz und Datensicherheit gelten dann, wenn im Rahmen der zu beauftragenden Leistung personenbezogene Daten verarbeitet werden. In diesem Fall ist der Auftraggeber als Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO und der Bieter als Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DSGVO einzuordnen, und die Parteien müssen deshalb gemäß Art. 28 Abs. 3 DSGVO in einem Vertrag oder einem anderen Rechtsinstrument die Verteilung der wesentlichen datenschutzrechtlichen Verpflichtungen regeln.[47] Insbesondere darf der Auftraggeber nur mit solchen Bietern zusammenarbeiten, die geeignete technische und organisatorische Maßnahmen so durchführen, dass die auftragsgegenständliche Datenverarbeitung im Einklang mit der Datenschutz-Grundverordnung steht und der Schutz der Rechte und Freiheiten der betroffenen Person gewährleistet ist.[48] Dies umfasst den Ausschluss der Datenverarbeitung zu eigenen Geschäftszwecken des Bieters, vgl. Art. 28 Abs. 10 DSGVO. Der Auftraggeber muss mithin bei Auswahl der in Betracht kommenden Bieter und gegebenenfalls Nachunternehmer die zu treffenden technischen und organisatorischen Maßnahmen überprüfen. Dabei geht es vor allem darum sicherzustellen, dass diese Maßnahmen in Erfüllung des Auftrags voraussichtlich ordnungsgemäß und dem Risiko angemessen implementiert werden, insbesondere im Fall grenzübergreifender Datenübermittlung. Diese Prüfung muss formal zwar erst vor Aufnahme der Verarbeitung personenbezogener Daten und damit regelmäßig nicht vor Zuschlagserteilung stattfinden;[49] aus praktischer Sicht sollte sie allerdings so früh wie möglich vorgenommen werden, um das Ergebnis noch im laufenden Vergabeverfahren berücksichtigen zu können. Art. 28 Abs. 2 DSGVO statuiert die Voraussetzungen für den Einsatz weiterer Auftragsverarbeiter.

39 Für den Abschluss des Auftragsverarbeitungsvertrages oder anderen Rechtsinstruments sind die formellen Voraussetzungen des Art. 28 Abs. 9 DSGVO („schriftlich") zu beachten. Besondere Sorgfalt ist hier geboten, sofern die Vereinbarung unmittelbar durch Zuschlag geschlossen werden soll.

f) Beispiele für Ansatzpunkte für datenschutzrechtliche Leistungsanforderungen

40 Im Folgenden sollen beispielhaft in Stichworten nicht abschließend mögliche Ansatzpunkte für die Beschaffung einer datenschutzkonformen Leistung dargestellt werden. Je nach gewünschter Ausgestaltung kann der Auftraggeber dabei jeweils sehr konkrete Festlegungen

[46] Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme vom 18. Mai 2021, BGBl. 2021 I S. 1122.

[47] Musterhafte Anhaltspunkte für den Inhalt einer entsprechenden Vereinbarung finden sich beispielsweise in Formblatt L 2441 des VHL Bayern, vgl. Fn. 7.

[48] Vgl. hierzu auch Formblatt L 2442 des VHL Bayern, vgl. Fn. 4.

[49] Hartung, in: Kühling/Buchner, DSGVO/BDSG, 3. Aufl. 2020, Art. 28 Rn. 60; Gabel/Lutz, in: Taeger/Gabel, DSGVO/BDSG/TTDSG, 4. Aufl. 2022, Art. 28 Rn. 27, 31.

treffen oder – unter Beachtung rechtlich oder sonst auftraggeberseitig zwingender Vorgaben – auch nur einen Rahmen für ein entsprechendes Ausgestaltungskonzept des späteren Auftragnehmers abstecken. Für öffentliche Stellen empfiehlt sich – auch unter dem Gesichtspunkt der Wahrung der Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO – die Formulierung möglichst konkreter datenschutzrechtlicher Anforderungen, um die datenschutzfreundlichste Leistung zu erhalten. So ist beispielsweise eine Wartung vor Ort aufgrund der damit verbundenen Überwachungsmöglichkeiten stets einer Fernwartung vorzuziehen.

Hinweis: Bei der Beschaffung vergessene und später auch nicht anderweitig umsetzbare datenschutzrechtliche Vorgaben können im schlechtesten Fall dazu führen, dass beispielsweise ein beschafftes IT-System nicht datenschutzkonform betrieben werden kann oder eine Dienstleistung nicht datenschutzkonform nutzbar ist. 41

- Allgemeine Darlegung der Ausgangslage beziehungsweise des Beschaffungsbedarfs, auch in datenschutzrechtlicher Hinsicht. 42
- Beschreibung der vorhandenen und der zu beschaffenden Betriebsumgebung, z. B.
  - auftraggeberseitig bereits vorhandene Hard- und Software;
  - Anforderungen an die zu beschaffende Hard- oder Software oder Dienstleistung;
  - Anpassbarkeit einer Werkskonfiguration an die auftraggeberseitigen Bedürfnisse der Datensicherheit und des Datenschutzes (z. B. Deaktivierung von Weitergabefunktionen oder Abschalten nicht benötigter Dienste und Schnittstellen);
  - Kompatibilität der zu beschaffenden Produkte mit bereits beim Auftraggeber eingesetzten Software- und Hardwareprodukten;
  - Erfordernis einer ständigen Netzanbindung zwischen Auftraggeber und Auftragnehmer für dauerhafte Zugriffe auf Systeme und/oder Ressourcen (z. B. durch Site-to-Site VPN);
  - Vorgaben zur Migration des Produktes oder der Dienstleistung in den Betrieb beim Auftraggeber (z. B. Erforderlichkeit der Unterbrechung bereits laufender Prozesse), gegebenenfalls Rollback-Strategie zur Wiederherstellung des vorherigen Zustands;
  - Verpflichtung des Auftragnehmers – auch betreffend den Datenschutz – stets die neueste Ausrüstung, Werkzeuge, Verfahren, Technologien, Updates und/oder Patches zur Verfügung zu stellen, einschließlich Vorgaben zur Umsetzung im laufenden Betrieb.
- Zutritts-, Zugangs- und Zugriffskontrolle, z. B.
  - Mandantenfähigkeit und Mandantentrennung (Anzahl der gewünschten unterschiedlichen Mandaten);
  - Berechtigungsmanagement (Benutzer- und Rechteverwaltung) unter Angabe der vom Auftraggeber gewünschten Anbindungen;
  - Sicherheit des Log-ins, z. B. Zwei-Faktor-Authentifizierung.

II. Erstellung der Vergabeunterlagen

- Datensicherheit und Wiederherstellung, z. B.
  - Verschlüsselung von Daten und des Transportwegs;
  - Verschlüsselungsmethoden entsprechend dem aktuellen Stand der Technik;
  - Sicherheitsanalyse (Penetrations- oder Schwachstellentests);
  - Geheimhaltungsverpflichtung (Non Disclosure Agreement) und/oder No-Spy-Erklärung.
- Verfügbarkeit der Daten, z. B.
  - Zuverlässigkeit und Ausfallsicherheit;
  - Konzept für den Ausfall von Systemen oder Produkten, z. B. Wiederanlaufzeiten, maximale Ausfallzeiten, Reaktionszeiten, Eskalationspfad.
- Spezifisch datenschutzrechtliche Leistungsbestandteile, z. B.
  - Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DSGVO mit Vorlagen;
  - Verzeichnis betreffend gemeinsame Verantwortlichkeit (Art. 26 DSGVO) und Auftragsdatenverarbeitung (Art. 28 DSGVO);
  - Umsetzung von Auskunfts- oder Löschbegehren;
  - Umsetzung der datenschutzrechtlichen Informations- und Auskunftspflichten;
  - Erstellung musterhafter Einwilligungserklärungen;
  - Erstellung von Datenschutzerklärungen für Webseiten;
  - Erstellung und Umsetzung von Datenschutz-Folgenabschätzungen;
  - Risikomanagement;
  - Design von datenschutzrechtlichen Workflows und Prozessen.
- Allgemein betreffend die Vertragsdurchführung, z. B.
  - Leistungsort;
  - Regelmäßige Berichterstattung und Termine, Berichtspflicht bei relevanten Änderungen / Notfällen;
  - Auswertungsmöglichkeiten, z. B. Dashboard;
  - Vereinbarung zur Auftragsdatenverarbeitung;
  - Kontrollrechte des Auftraggebers;
  - Schadensersatz und Vertragsstrafen bei Nicht- oder Schlechterfüllung der Leistung.

- Service (Service Level Agreement), z. B.

  Festlegung gewünschter Servicezeiten durch den Auftraggeber, z. B. 24/7 Bereitschaft.

- Wartung, z. B.

  - Fernwartung oder Wartung vor Ort mit jeweils entsprechenden Vorgaben zur Wahrung des Datenschutzes und der Datensicherheit;
  - Festlegung von Wartungsfenstern;
  - Gewährleistung der Zuverlässigkeit der Wartungsmittel, z. B. durch Ausgabe von speziellen Wartungslaptops durch den Auftraggeber.

- Schulungen, z. B.

  - Vorgaben betreffend Schulungsbedarf beim Auftraggeber, z. B. Bereitstellung einer E-Learning-Plattform;
  - Verpflichtung zu regelmäßiger Aus- und Weiterbildung des Personals auf Seiten des Dienstleisters.

- Fremdpersonal / Subunternehmer, z. B.

  Vorgaben zur Zulässigkeit des Einsatzes von Fremdpersonal und/oder Subunternehmern beim Auftragnehmer, einschließlich Wechsel von Subunternehmern.

- Vertragsbeendigung, z. B.

  - Laufzeit und Kündigungsrechte beziehungsweise -pflichten;
  - Pflichten nach Vertragsbeendigung, z. B. Datenübergabe, Aufbewahrungspflichten, Löschpflichten, Entfernung nicht mehr benötigter Berechtigungen beziehungsweise Freigaben;
  - möglichst Vermeidung der Vendor-Lock-in-Problematik.[50]

2. Datenschutzkonforme Vertragsbedingungen

Teil der vom Auftraggeber im Vergabeverfahren zur Verfügung zu stellenden Vertragsunterlagen sind neben der Leistungsbeschreibung die Vertragsbedingungen, § 29 Abs. 1 Nr. 3 VgV. Auch diese müssen datenschutzkonform festgelegt werden. Die Vertragsbedingungen **43**

[50] Der Wirtschaftsbegriff bezeichnet ein Leistungsverhältnis, bei dem Kunden derart von Produkten oder Dienstleistungen eines Anbieters abhängig sind, dass der Wechsel zu einem Mitbewerber mit hohem Aufwand und hohen Kosten verbunden wäre und deshalb in der Regel unterbleibt. Entscheidend sind dabei meist technische, prozessuale oder vertragliche Abhängigkeiten zwischen einzelnen Produkten oder Leistungsteilen des Anbieters, die auf diese Weise ein mehr weniger in sich geschlossenes System bilden.

lassen sich in die genuin vertraglichen Regelungen sowie die sog. Ausführungsbedingungen unterteilen.

44 Wesentliche Anhaltspunkte für die Abfassung der **vertraglichen Regelungen** finden sich nicht nur in den EVB-IT und Art. 28 Abs. 3 DSGVO, sondern insbesondere in den oben bereits angesprochenen Standardvertragsklauseln (SCC). Die SCC müssen gegebenenfalls einzelfallbezogen durch zusätzliche vertragliche Vereinbarungen ergänzt werden;[51] Änderungen an deren verbindlichen Teil sind weder durch den öffentlichen Auftraggeber noch durch einen Bieter möglich.[52]

45 Konkret bezogen auf die Ausführung des Auftrags statuiert **§ 128 Abs. 1 GWB** die gesetzliche Vorgabe für die Unternehmen, alle für sie geltenden rechtlichen Verpflichtungen einzuhalten. Dies umfasst **alle zwingenden Rechtsvorschriften** und damit auch die zwingenden Teile der Datenschutz-Grundverordnung.[53] Ein Verstoß gegen diese rechtlichen Verpflichtungen kann unterhalb der Strafbarkeitsschwelle[54] einen fakultativen Ausschlussgrund vom Vergabeverfahren im Sinne des § 124 Abs. 1 GWB, § 57 Abs. 1 VgV wegen mangelnder Eignung begründen; Verstöße gegen datenschutzrechtliche Bestimmungen können dabei eine „nachweisliche schwere Verfehlung im Rahmen der beruflichen Tätigkeit" darstellen, § 124 Abs. 1 Nr. 3 GWB. Ebenso kommt bei Nichteinhaltung von zwingenden Datenschutzvorgaben ein Ausschluss gemäß §§ 53 Abs. 7, 57 Abs. 1 Nr. 4 VgV wegen Änderung der Vergabeunterlagen in Betracht.[55]

46 Darüber hinaus können öffentliche Auftraggeber gemäß **§ 128 Abs. 2 GWB** in der Auftragsbekanntmachung oder den Vergabeunterlagen besondere Bedingungen für die Ausführung eines Auftrags (**Ausführungsbedingungen**) festlegen. Es handelt sich hierbei um Vertragsbedingungen, die dem späteren Auftragnehmer zwingend zur Beachtung und Einhaltung vorgegeben werden. Anders als bei den Zuschlagskriterien findet insoweit keine Wertung statt; ist ein Bewerber oder Bieter nicht willens oder in der Lage, diese Bedingungen im Fall der Zuschlagserteilung bei der Auftragsausführung zu beachten, liegt kein zuschlagsfähiges Angebot vor, §§ 53 Abs. 7, 57 Abs. 1 Nr. 4 VgV. Die zwingenden Ausführungsbedingungen werden daher auch als „**Ausschlusskriterien**" oder „A-Kriterien" bezeichnet. Erfüllt der bezuschlagte Auftragnehmer die Ausführungsbedingungen während der Erbringung der Leistung nicht, liegt eine Vertragsverletzung vor, die zivilrechtliche Konsequenzen nach sich ziehen

[51] EuGH, Urteil vom 16. Juli 2020, C-311/18 (Schrems II).

[52] Vgl. Klausel 2 Anhang des Durchführungsbeschlusses der Kommission über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates, 4. Juni 2021, C(2021) 3972 final, sowie Klausel 2 Anhang des Durchführungsbeschlusses der Kommission über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates und Artikel 29 Absatz 7 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates, 4. Juni 2021, C(2021) 3701 final.

[53] Die auftraggeberseitige Vorgabe der softwaretechnischen Einhaltung der Datenschutz-Grundverordnung als Ausführungsbedingung im Sinne des § 128 Abs. 2 GWB ergibt daher keinen echten Sinn. So aber VK Baden-Württemberg, Beschluss vom 13. Juli 2022, 1 VK 23/22, BeckRS 2022, 18405.

[54] Bei Vorliegen einer der in § 123 GWB genannten Straftaten ist der Ausschluss vom Vergabeverfahren zwingend.

[55] VK Südbayern, Beschluss vom 8. Februar 2023, 3194.Z3-3_01-22-42, IBRRS 2023, 0880.

kann, bei entsprechender Vereinbarung sogar in Gestalt von Vertragsstrafen oder Sonderkündigungsrechten.

Voraussetzung für die wirksame Festlegung von Ausführungsbedingungen ist gemäß § 128 Abs. 2 Satz 1 GWB, dass diese mit dem Auftragsgegenstand entsprechend § 127 Abs. 3 GWB in Verbindung stehen; einer gesonderten Begründung des öffentlichen Auftraggebers bedarf es nicht. Die Ausführungsbedingungen können insbesondere wirtschaftliche, innovationsbezogene, umweltbezogene, soziale oder beschäftigungspolitische Belange oder den Schutz der Vertraulichkeit von Informationen umfassen, § 128 Abs. 2 Satz 3 GWB; diese Aufzählung ist nicht abschließend. Denkbar sind beispielsweise Vorgaben zur Beachtung internationaler Standards wie der ILO-Kernarbeitsnormen[56] oder zu Maßnahmen zur Förderung der Gleichstellung von Frauen und Männern am Arbeitsplatz.[57] Von besonderer datenschutzrechtlicher Bedeutung können unter anderem die Abgabe einer sog. „No-Spy-Erklärung"[58] oder der Ausschluss von US-Unternehmen in der Lieferkette[59] sein. **47**

3. Datenschutzrechtliche Anforderungen als Bewerbungsbedingungen

Datenschutz kann im Vergabeverfahren allerdings nicht nur auf der Ebene der Vertragsunterlagen, sondern auch im Zusammenhang mit den Bewerbungsbedingungen im Sinne des § 29 Abs. 1 Nr. 2 VgV als Kriterium berücksichtigt werden. Dies umfasst insbesondere die Eignungs- und Zuschlagskriterien. **48**

a) Datenschutzrechtliche Anforderungen als Eignungskriterien

Dabei gilt allerdings zu beachten, dass die Festlegung datenschutzrechtlicher Vorgaben in Form von **Eignungskriterien nur eingeschränkt** möglich ist: **49**

§ 122 Abs. 1 GWB statuiert zwar den Grundsatz, dass öffentliche Aufträge an fachkundige und leistungsfähige Unternehmen vergeben werden, die nicht nach den §§ 123 oder 124 GWB ausgeschlossen sind. Die vom Auftraggeber zur ordnungsgemäßen Ausführung des Auftrags festgelegten Kriterien, mithin die Eignungskriterien, dürfen nach § 122 Abs. 2 Satz 2 GWB jedoch nur die Befähigung und Erlaubnis zur Berufsausübung, die wirtschaftliche und **50**

[56] Erwägungsgrund 98 Richtlinie 2014/24/EU.

[57] Erwägungsgrund 98 Richtlinie 2014/24/EU.

[58] Unter einer „No-Spy-Erklärung" versteht man die Eigenerklärung des Bewerbers oder Bieters, keiner Verpflichtung zu unterliegen, im Auftragsfall vertrauliche Informationen Dritten zugänglich machen zu müssen. Ausgenommen sind danach gesetzliche Offenlegungspflichten, es sei denn, solche Offenlegungspflichten bestünden gegenüber ausländischen Sicherheitsbehörden. Vgl. „No-Spy-Erlass" des Bundesministeriums des Innern und für Heimat mit ergänzender Handreichung vom 19. August 2014, Internet: https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2014/08/no-spy-erlass.html. Beachte auch OLG Düsseldorf, Beschluss vom 21. Oktober 2015, VII-Verg 28/14, BeckRS 2015, 18210; BKartA, Beschluss vom 24. Juni 2014, VK 2-39/14, ZfBR 2014, 787.

[59] Rath/Keller, US Cloud-Anbieter, der „Risikofaktor US CLOUD Act", das Vergaberecht und die Nachfrage nach sicheren Sovereign Clouds, CR 2022, 682, 683.

finanzielle Leistungsfähigkeit sowie die technische und berufliche Leistungsfähigkeit betreffen. Denn mittels der Eignungskriterien soll festgestellt werden, ob ein Unternehmen nach den ihm zurechenbaren[60] generellen Fähigkeiten und Fertigkeiten in der Lage sein wird, den Auftrag auszuführen.[61] Insoweit unterscheidet sich die Eignung auch von den Zuschlagskriterien, die sich auf die angebotene Leistung, also den konkreten Auftrag, beziehen und mit der Ermittlung des wirtschaftlichsten Angebots zusammenhängen. Eignungsprüfung und wirtschaftliche Bewertung der Angebote sind voneinander zu trennen und dürfen nicht miteinander vermischt werden.[62]

51 §§ 44 ff. VgV zählen – zum Teil abschließend[63] – die Belege auf, die zum Nachweis solcher Eignungskriterien herangezogen werden können. Die Festlegung von Kriterien betreffend den allgemeinen datenschutzrechtlichen status quo der am Auftrag interessierten Unternehmen ist dabei nur im Zusammenhang mit der **technischen und beruflichen Leistungsfähigkeit** nach § 46 VgV denkbar, so zum Beispiel

- **§ 46 Abs. 3 Nr. 1 VgV geeignete Referenzen:** Eigenerklärung über eine bestimmte Anzahl nachweisbarer Referenzen mit Vertragsdetails und Kontaktdaten, in denen ein Unternehmen als externer Datenschutzbeauftragter bestellt ist oder wo das Unternehmen bei einem öffentlichen Auftraggeber die Einführung des Datenschutzes begleitet hat;
- **§ 46 Abs. 3 Nr. 6 VgV Studien- und Ausbildungsnachweise sowie Bescheinigungen über die Erlaubnis zur Berufsausübung:** Nachweis der fachlichen Qualifikation, Ausbildung und Berechtigung des Datenschutzbeauftragten nach Art. 37 DSGVO/Nachweis über eine bestimmte Anzahl an Fortbildungsseminaren im Datenschutz/Nachweis der Berechtigung zur Durchführung von Prüfungen nach § 8a Gesetz über das Bundesamt für Sicherheit in der Informationstechnik.

52 Konkrete Vorgaben zum Leistungsort können dagegen nicht als Eignungskriterium gestaltet werden, da sie nicht allgemein unternehmensbezogen sind. Für datenschutzrelevante Beschaffungen könnte der Auftraggeber im Rahmen der Eignungsprüfung allenfalls Angaben dazu fordern, ob das Unternehmen des Bewerbers oder Bieters grundsätzlich organisatorisch in der Lage ist, „personenbezogene Daten nur an sicheren Orten zu verarbeiten". Diese Abfrage enthält jedoch keine Aussage zum Ort der Leistungserbringung im Auftragsfall. Wie gesehen (siehe Rn. 25 ff.), sind Vorgaben zum Leistungsort vielmehr Teil der Leistungsbeschreibung.

[60] Eignungsanforderungen sind bieterbezogen. Daher dürfen ausschließlich Sachverhalte berücksichtigt werden, die dem Bewerber/Bieter in irgendeiner Form zurechenbar sind. Dies sind regelmäßig nur solche Umstände, auf die ein Bewerber/Bieter Einfluss nehmen kann. Ergeben sich aus der Rechtsordnung eines Landes, der ein Bewerber/Bieter unterworfen ist, bestimmte Verpflichtungen, denen er sich nicht entziehen kann, ist es unzulässig, diese als ein die Eignung ausschließendes oder in Frage stellendes Fehlverhalten anzusehen. Dies gilt auch dann, wenn der Bewerber/Bieter infolge der nationalen Verpflichtungen zwangsläufig gegen die Vorgaben einer anderen Rechtsordnung verstoßen muss, BKartA, Beschluss vom 24. Juni 2014, VK 2-39/14, ZfBR 2014, 787.

[61] BKartA, Beschluss vom 13. Juni 2014, VK 1-34/14, IBRRS 2014, 2469.

[62] Grundlegend EuGH, Urteil vom 20. September 1988, C-31/87, und Urteil vom 24. Januar 2008, C-532/06; BGH, Urteil vom 15. April 2008, X ZR 129/06, BeckRS 2008, 10415.

[63] OLG Düsseldorf, Beschluss vom 7. Mai 2014, VII-Verg 46/13, ZfBR 2014, 785 m. w. N.

Bei Nichteinhaltung der Eignungsanforderungen sind die zwingenden und fakultativen Ausschlussgründe der §§ 123, 124 GWB in Verbindung mit § 57 Abs. 1 VgV unter Einbeziehung der Möglichkeit zur Selbstreinigung nach § 125 GWB zu berücksichtigen. 53

b) Datenschutzrechtliche Anforderungen als Wertungskriterien

Uneingeschränkt möglich, in der Praxis allerdings durchaus komplex, ist die Bewertung datenschutzrechtlicher Anforderungen als Zuschlagskriterien, auch sog. „**Bewertungskriterien**“ oder „B-Kriterien“. Der Zuschlag wird gemäß § 127 Abs. 1 Satz 1 GWB auf das wirtschaftlichste Angebot erteilt, welches sich nach dem besten Preis-Leistungs-Verhältnis bestimmt, § 127 Abs. 1 Satz 3 GWB. Zu dessen Ermittlung können nach § 127 Abs. 1 Satz 4 GWB in Verbindung mit § 58 Abs. 2 VgV neben dem Preis oder den Kosten auch qualitative, umweltbezogene oder soziale Aspekte herangezogen werden, vorausgesetzt, diese stehen mit dem Auftragsgegenstand in Verbindung, § 127 Abs. 3 Satz 1 GWB. Die Zuschlagskriterien, einschließlich eventueller Unterkriterien,[64] und deren Gewichtung müssen transparent, nicht diskriminierend und willkürfrei festgelegt und in der Auftragsbekanntmachung oder den Vergabeunterlagen aufgeführt werden, § 127 Abs. 4 Satz 1, Abs. 5 GWB in Verbindung mit § 58 Abs. 3 VgV. Für die Preisgestaltung setzt dies eine detaillierte Kostenaufschlüsselung voraus. 54

In der Wertungsphase nimmt der Auftraggeber eine Bewertung der Angebote dahingehend vor, ob und inwieweit jeweils die vorgegebenen Zuschlagskriterien erfüllt sind, § 127 Abs. 1 Satz 2 GWB. Die Bewertung erfolgt dabei in der Regel anhand von Punkten, die den Erfüllungsgrad der vom Auftraggeber aufgestellten Anforderungen widerspiegeln. Der Auftraggeber hat insoweit einen Beurteilungsspielraum. Dieser kann von den Nachprüfungsinstanzen nur dahin überprüft werden, ob das vorgeschriebene Verfahren eingehalten wurde, von einem zutreffenden und vollständig ermittelten Sachverhalt ausgegangen wurde, keine sachwidrigen Erwägungen für die Entscheidung herangezogen wurden und nicht gegen allgemein gültige Bewertungsansätze wie beispielsweise das Gleichbehandlungsgebot (§ 97 Abs. 2 GWB)[65] verstoßen wurde.[66] 55

Spezifisch den Datenschutz betreffend können über die Einhaltung der Vorgaben der Datenschutz-Grundverordnung als Mindeststandard im Sinne des § 128 Abs. 1 GWB hinausgehende Maßnahmen des Bieters im Zusammenhang mit Datenverarbeitung wertend berücksichtigt werden. Diese können sich unter anderem auf bestimmte Funktionalitäten oder Leistungskennzahlen von Hard- und Software, Softwareentwicklung oder Implementierung von IT-Lösungen und Projektmanagement beziehen.[67] Denkbar scheint auch die wertende Berücksichtigung von über die Vorgaben der Datenschutz-Grundverordnung hinausgehenden technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten. In der Praxis bedeutet dies nicht nur, dass die einschlägigen Wertungskriterien und deren Ge- 56

64 EuGH, Urteil vom 24. November 2005, C-331/04.

65 BGH, Beschluss vom 4. April 2017, X ZB 3/17, BeckRS 2017, 109172.

66 Kling, in: Immenga/Mestmäcker, Wettbewerbsrecht, 6. Aufl. 2021, § 127 GWB Rn. 25 ff.; Renner, in: Pünder/Schellenberg, Vergaberecht, 3. Aufl. 2019, § 127 GWB Rn. 19.

67 UfAB 2018 (Fn. 25), S. 580.

wichtung vorab ausgearbeitet und bekannt gemacht werden müssen. Anschließend muss zudem deren Umsetzung vom Auftraggeber anhand der von den Bietern eingereichten Unterlagen wertend geprüft werden. Bei Einforderung entsprechend umfassender Konzepte können sich diese Prüfung und deren Dokumentation mit Blick auf die (technische und rechtliche) Bewertung betreffend den Grad der Erfüllung der gestellten Anforderungen, die Nachvollziehbarkeit und die erforderliche Gleichbehandlung durchaus komplex gestalten. Von der Rechtsprechung als Wertungskriterium anerkannt wurden beispielsweise DSGVO-konforme softwaretechnische Möglichkeiten zur Berechtigungssteuerung verbunden mit der Vorgabe, Daten ausschließlich in einem EU-/EWR-Rechenzentrum zu verarbeiten, bei dem kein Nachunternehmen/Konzernunternehmen in Drittstaaten ansässig ist,[68] ebenso die Vorlage eines Datenschutzkonzepts, auf dessen Grundlage gewährleistet sein soll, dass die Leistung des Bieters den Anforderungen der datenschutzrechtlichen Regulierungen entspricht und persönliche Daten bestmöglich geschützt sind.[69]

4. Subunternehmer

57 Die obigen Ausführungen gelten beim Einsatz von Subunternehmern (auch „Unterauftragnehmern“) entsprechend. Der Auftraggeber kann Vorgaben zur Zulässigkeit des Einsatzes von Subunternehmern bei den Bewerbern oder Bietern, einschließlich deren Wechsel, machen. Die Bewerber oder Bieter müssen für die von ihnen eingeschalteten Subunternehmer einstehen und sich deren Leistungsteil und gegebenenfalls deren Eignung (sog. „Eignungsleihe“, § 47 VgV) zurechnen lassen, denn diese sind Bestandteil ihrer Teilnahmeanträge beziehungsweise Angebote, § 36 VgV.

[68] VK Baden-Württemberg, Beschluss vom 13. Juli 2022, 1 VK 23/22, BeckRS 2022, 18405.

[69] VK Südbayern, Beschluss vom 8. Februar 2023, 3194-Z3-3_01-22-42, IBRRS 2023, 0880.

III. Konkrete Umsetzung im Vergabeverfahren, insbesondere Verfahrenswahl

1. Verfahrenswahl

Oberhalb der EU-Schwellenwerte[70] gelingt die Berücksichtigung datenschutzrechtlicher Kriterien am praktikabelsten im Rahmen eines Verhandlungsverfahrens mit Teilnahmewettbewerb nach § 119 Abs. 5 GWB in Verbindung mit §§ 14 Abs. 3, 17 VgV oder eines wettbewerblichen Dialogs nach § 119 Abs. 6 GWB in Verbindung mit §§ 14 Abs. 3, 18 VgV. Diese Verfahren können für sämtliche Formen von Liefer- und Dienstleistungen durchgeführt werden und gelten insbesondere auch für freiberufliche Leistungen im Sinne von § 18 Abs. 1 Nr. 1 Einkommensteuergesetz,[71] §§ 1, 2 VgV in Verbindung mit § 115 GWB. **58**

Zulässig sind diese Vergabearten in Abweichung vom Grundsatz des offenen beziehungsweise nicht offenen Verfahrens (§ 119 Abs. 2 GWB) ausweislich § 14 Abs. 3 VgV im Wesentlichen immer dann, wenn die Leistungsanforderungen nicht hinreichend vom Auftraggeber selbst beschreibbar sind[72] beziehungsweise der Auftrag aufgrund konkreter Umstände nicht ohne vorherige Verhandlungen vergeben werden kann.[73] Besondere Bedeutung haben die beiden Verfahren daher insbesondere bei Liefer- oder Dienstleistungen, die konzeptionelle oder innovative Lösungen erfordern[74] und somit keine Standardleistungen zum Gegenstand haben, die von vielen Marktteilnehmern erbracht werden können.[75] Aufgrund der Vielzahl an Möglichkeiten, durch Maßnahmen und/oder Regelungen eine datenschutzkonforme Leistungserbringung darzustellen, sind die Voraussetzungen des § 14 Abs. 3 VgV mithin erfüllt. Offenes und nicht offenes Verfahren bieten dem Auftraggeber dagegen keinen Gestaltungs- oder Verhandlungsspielraum. **59**

Beide Verfahren gewährleisten auch insofern eine besonders interessengerechte Umsetzung, als sie eine **„Aufgliederung" der einzelnen Verfahrensschritte** ermöglichen: So kann **60**

[70] Die Schwellenwerte für unionsweite Vergabeverfahren werden alle zwei Jahre von der Europäischen Union überprüft und im Regelfall auch angepasst. Der jeweilige Schwellenwert für Liefer- und Dienstleistungen ergibt sich aus Art. 4 Richtlinie 2014/24/EU in der jeweils geltenden Fassung und wird im Amtsblatt der EU bekannt gegeben. Seit 1. Januar 2022 liegt der EU-Schwellenwert für Liefer- und Dienstleistungsaufträge bei 214.000,– EUR netto.

[71] Für Architekten- und Ingenieurleistungen sind allerdings die Sonderregelungen der §§ 73 ff. VgV zu beachten.

[72] § 14 Abs. 3 Nr. 4 VgV.

[73] § 14 Abs. 3 Nr. 3 VgV.

[74] § 14 Abs. 3 Nr. 2 VgV.

[75] Vgl. die Begründung zu § 14 Abs. 3 VgV, BR-Drs. 87/16, S. 168 mit Verweis auf Erwägungsgrund 43 der Richtlinie 2014/24/EU.

der Auftraggeber zunächst im Rahmen des Teilnahmewettbewerbs abschließend[76] die Eignung der Unternehmen prüfen (sog. Präqualifikationsphase)[77] und anschließend nur eine begrenzte Anzahl der so qualifizierten Bewerber zur Angebotsabgabe beziehungsweise zum Dialog auffordern. Für die **Begrenzung der Teilnehmerzahl** nach Präqualifizierung gilt dabei zu beachten, dass diese gemäß § 51 Abs. 1 VgV ausschließlich mittels objektiver und nichtdiskriminierender Eignungskriterien vorzunehmen ist, welche aus Transparenzgründen bereits in der Auftragsbekanntmachung oder der Aufforderung zur Interessensbestätigung anzugeben sind. Erforderlichenfalls muss der Auftraggeber eine – ebenfalls bekanntzugebende – Eignungsmatrix aufsetzen.[78] Für die Auswahl unter einer größeren Anzahl an grundsätzlich geeigneten Bewerbern kommt es dann auf den Grad der Eignung für die konkret zu vergebende Leistung an; hierfür können insbesondere Eignungskriterien herangezogen werden, die die zu erwartende Qualität der Auftragsausführung betreffen.[79] Eine solche Gewichtung verstößt nicht gegen den Grundsatz „kein Mehr an Eignung".[80] Der Auftraggeber muss vorab eine Mindest- und gegebenenfalls auch Höchstzahl der aufzufordernden Bewerber festlegen, § 51 Abs. 1 Satz 2 VgV; diese darf gemäß § 51 Abs. 2 Satz 1 VgV beim Verhandlungsverfahren und wettbewerblichen Dialog nicht niedriger als drei sein.

61 Die Verfahren unterscheiden sich durch Zeitpunkt und Zielsetzung der Einbeziehung der Unternehmen. Beide Verfahren können allerdings insofern zu einer Stärkung des Datenschutzes beitragen, als gegebenenfalls im Rahmen der Verhandlungen beziehungsweise des wettbewerblichen Dialogs innerhalb des vom Auftraggeber festgelegten Leistungsrahmens möglichst datenschutzfreundliche Leistungen „erarbeitet" werden können – auch solche, an die der Auftraggeber selbst nicht gedacht hat.

a) Verhandlungsverfahren mit Teilnahmewettbewerb

62 Spezifikum des Verhandlungsverfahrens mit Teilnahmewettbewerb nach § 119 Abs. 5 GWB in Verbindung mit §§ 14 Abs. 3, 17 VgV ist die Verhandlungsphase, die nach Einreichung der Erstangebote durch die im Rahmen des Teilnahmewettbewerbs ausgewählten Bieter eröffnet wird und mit der Aufforderung zur Abgabe der endgültigen Angebote endet. Erst nach Auswahl durch den Auftraggeber müssen die Bieter ein Angebot für die ausgeschriebene Leistung abgeben und Ausführungen zu den als Zuschlagskriterien festgelegten Aspekten machen, beispielsweise durch Vorlage eines Datenschutzkonzepts. Anschließend wird über

[76] Eine erneute Überprüfung der Eignung der zur Angebotsabgabe aufgeforderten Bewerber findet nur statt, sofern sich über den Verlauf des Vergabeverfahrens Umstände ergeben, die die festgestellte Eignung entfallen lassen könnten, BGH, Beschluss vom 7. Januar 2014, X ZB 15/13, BeckRS 2014, 2188.

[77] Die Interessenten können die Eignungsnachweise dabei einzelauftragsbezogen erbringen oder ihre Fachkunde und Leistungsfähigkeit mittels einer sog. Präqualifzierung unabhängig von einer konkreten Ausschreibung vorab nachweisen. Die Präqualifizierung erspart, regelmäßig in Vergabeverfahren verlangte Einzelnachweise bei jeder Ausschreibung neu vorlegen zu müssen, da öffentliche Auftraggeber die von Präqualifizierungsstellen hinterlegten Sammelbescheinigungen anstelle der Einzelnachweise anerkennen können.

[78] Pünder/Klafki, in: Pünder/Schellenberg, Vergaberecht, 3. Aufl. 2019, § 51 VgV Rn. 7.

[79] Pünder/Klafki, in: Pünder/Schellenberg, Vergaberecht, 3. Aufl. 2019, § 51 VgV Rn. 5.

[80] BGH, Urteil vom 16. Oktober 2001, X ZR 100/99, BeckRS 2001, 9163; OLG Düsseldorf, Beschluss vom 20. Juli 2015, VII-Verg 37/15, BeckRS 2015, 14053; VK Rheinland-Pfalz, Beschluss vom 22. Juni 2012, VK 1-15/12, juris.

diese Angebote verhandelt mit dem Ziel, die Angebote inhaltlich zu verbessern, damit – gegebenenfalls auch unter Änderung der Vergabeunterlagen innerhalb der zulässigen Grenzen (§ 17 Abs. 10 und 13 VgV) – die Liefer- und Dienstleistungen letztlich genau auf den konkreten Bedarf des Auftraggebers zugeschnitten sind. Unter Einhaltung des Gleichbehandlungs- und Transparenzgebots dürfen die Verhandlungen daher grundsätzlich den gesamten Angebotsinhalt mit Ausnahme der in den Vergabeunterlagen festgelegten Mindestanforderungen und Zuschlagskriterien umfassen.

b) Wettbewerblicher Dialog

Die Durchführung eines wettbewerblichen Dialogs nach § 119 Abs. 6 GWB in Verbindung mit §§ 14 Abs. 3, 18 VgV bietet sich für die Konstellation an, dass ein Auftraggeber seine Bedürfnisse und Anforderungen an die zu beschaffende Leistung noch nicht abschließend geklärt hat und diese im Dialog mit Unternehmen eruieren und erörtern will. **63**

Der wettbewerbliche Dialog gliedert sich in den Teilnahmewettbewerb, die sog. Dialogphase und die Angebotsphase. Verhandlungen sind nur mit dem zu bezuschlagenden Bieter und nur in den engen Grenzen des § 18 Abs. 9 VgV möglich. **64**

c) Verhandlungsverfahren ohne Teilnahmewettbewerb

Davon zu unterscheiden ist das Verhandlungsverfahren ohne Teilnahmewettbewerb nach § 119 Abs. 5 GWB in Verbindung mit § 17 Abs. 5 VgV, das wegen der damit verbundenen weitreichenden Wettbewerbsbeschränkung nur in den eng auszulegenden Ausnahmetatbeständen des § 14 Abs. 4 VgV zulässig ist. Für informationstechnische Leistungen kommen hier insbesondere die Ausnahmen des § 14 Abs. 4 Nr. 2 Buchst. b oder c VgV in Betracht, wenn aus technischen Gründen kein Wettbewerb vorhanden ist und damit faktisch eine Monopolstellung besteht, oder der Schutz von ausschließlichen Rechten, insbesondere von gewerblichen Schutzrechten, dazu führt, dass der Auftrag nur von einem bestimmten Unternehmen durchgeführt werden kann. Als zusätzliche Voraussetzung gilt nach § 14 Abs. 6 VgV in diesen Fällen außerdem, dass keine vernünftige Alternative oder Ersatzlösung vorhanden sein darf und der mangelnde Wettbewerb insbesondere nicht das Ergebnis einer künstlichen Einschränkung der Auftragsvergabeparameter sein darf. **65**

Die Durchführung des Verhandlungsverfahrens ohne Teilnahmewettbewerb entspricht – mit Ausnahme der Ausführungen zum Teilnahmewettbewerb – den Hinweisen unter Rn. 62 zum Verhandlungsverfahren mit Teilnahmewettbewerb. Es kommt im Gegensatz zu diesem allerdings nur in Betracht, wenn der Auftraggeber eine sehr spezifische Leistung beschaffen möchte, da nur in diesem Fall die Ausnahmetatbestände des § 14 Abs. 4 VgV überhaupt hinreichend begründet werden können. **66**

d) Vergabeverfahren unterhalb der EU-Schwellenwerte

Liegt der geschätzte Auftragswert der auszuschreibenden Leistung unterhalb der EU-Schwellenwerte, gelten die nationalen Vergabevorschriften. So findet für Liefer- und Dienst- **67**

leistungen die Verfahrensordnung für die Vergabe öffentlicher Liefer- und Dienstleistungsaufträge unterhalb der EU-Schwellenwerte (UVgO) Anwendung. Freiberufliche Leistungen sind hiervon dagegen ausgenommen; für diese gelten im Unterschwellenbereich nur das Wettbewerbsgebot nach § 50 UVgO sowie die Grundsätze der Wirtschaftlichkeit und Sparsamkeit des Art. 7 Abs. 1 Bayerische Haushaltsordnung.

68 Die obigen Ausführungen zum bei datenschutzrelevanten Leistungen oftmals erforderlichen Gestaltungs- und Verhandlungsspielraum treffen auch auf nationale Vergaben zu, sodass für die Vergabe von Liefer- oder Dienstleistungen insbesondere die Verhandlungsvergabe mit oder ohne Teilnahmewettbewerb gemäß § 8 Abs. 4 in Verbindung mit § 12 UVgO in Betracht kommt. Bei Vorliegen der entsprechenden Voraussetzungen stehen diese dem öffentlichen Auftraggeber nach seiner Wahl zu Verfügung.

2. Rahmenvereinbarungen

69 Generell ist für informationstechnische Leistungen in Abweichung von der Einzelbeschaffung die Ausschreibung einer Rahmenvereinbarung häufig die flexiblere und effizientere und daher vorzugswürdigere Variante, da bei richtiger Vorgehensweise der eigene Bedarf über einen längeren Zeitraum gedeckt werden kann. Spezifische Vorgaben hierzu machen § 103 Abs. 5 GWB in Verbindung mit § 21 VgV beziehungsweise § 15 UVgO. Die Laufzeit von Rahmenvereinbarungen ist auf höchstens vier (§ 21 Abs. 6 VgV) beziehungsweise sechs (§ 15 Abs. 4 UVgO) Jahre beschränkt. Ein besonderes Augenmerk ist auf die vorab vorzunehmende Auftragswertschätzung zu legen: Gemäß § 3 Abs. 4 VgV errechnet sich diese bei Rahmenvereinbarungen auf der Grundlage des geschätzten Gesamtwertes aller Einzelaufträge, die während der gesamten Laufzeit der Rahmenvereinbarung geplant sind. Deren Validität ist gerade bei informationstechnischen Leistungen mit fluktuierendem Bedarf nicht unproblematisch und mit dem Risiko behaftet, dass eine erhebliche Überschreitung der ursprünglich geschätzten Abnahmemenge als wesentliche Vertragsänderung im Sinne des § 132 Abs. 1 GWB einzuordnen ist.[81] In diesem Fall ist gemäß § 132 Abs. 1 Satz 1 GWB ein neues Vergabeverfahren durchzuführen, sofern nicht einer der Ausnahmetatbestände des § 132 Abs. 2 oder 3 GWB Anwendung findet. Nicht erforderlich ist demgegenüber die Angabe von Mindestabnahmemengen oder die Festlegung von Obergrenzen; eine Konkretisierung erfolgt erst bei den Einzelabrufen, vgl. Art. 33 Abs. 1 UAbs. 2 a. E. und Art. 49 in Verbindung mit Anhang V Teil C Nr. 10a Richtlinie 2014/24/EU sowie § 21 Abs. 1 Satz 2 VgV.[82] Im Übrigen gelten für Rahmenvereinbarungen dieselben Beschaffungsgrundsätze wie oben, insbesondere auch hinsichtlich der Verfahrenswahl.

[81] A. A Koch, Flexibilität von Rahmenvereinbarungen bei IT-Beschaffungen, MMR 2020, 213, 215 f., der die Anwendbarkeit des § 132 GWB nur bei Festlegung einer Obergrenze für den Rahmenvertrag bejahen möchte.

[82] Zum Ganzen BKartA, Beschluss vom 19. Juli 2019, VK 1-39/19, BeckRS 2019, 19883, unter Auseinandersetzung mit EuGH, Urteil vom 19. Dezember 2018, C-216/17 zur alten Rechtslage nach Richtlinie 2004/18/EG des Europäischen Parlaments und des Rates vom 31. März 2004 über die Koordinierung der Verfahren zur Vergabe öffentlicher Bauaufträge, Lieferaufträge und Dienstleistungsaufträge.

3. Prüfpflicht des Auftraggebers

Im Zusammenhang mit der Durchführung des Vergabeverfahrens stellt sich auch die Frage, in welcher Form und in welchem Umfang der Auftraggeber zur Überprüfung der von Bewerbern oder Bietern im Vergabeverfahren gemachten Angaben verpflichtet ist. Dabei genügen nach herrschender Auffassung in Übereinstimmung mit Art. 67 Abs. 4 Richtlinie 2014/24/EU aus vergaberechtlicher Sicht grundsätzlich Eigenerklärungen des Bewerbers oder Bieters, in denen er sich auf die Einhaltung bestimmter Maßnahmen verpflichtet; deren Überprüfung vom Auftraggeber ist in aller Regel nur angezeigt, sofern substanzielle Zweifel an den Angaben bestehen.[83] **70**

Im Zusammenhang mit der Ausschreibung datenschutzrelevanter Leistungen trifft den Auftraggeber als den datenschutzrechtlich Verantwortlichen allerdings als Ausfluss seiner Rechenschaftspflicht nach **Art. 5 Abs. 2 DSGVO**, welche sich auch auf den Verarbeitungsgrundsatz der Rechtmäßigkeit gemäß Art. 5 Abs. 1 Buchst. a DSGVO bezieht, eine **umfangreiche Prüfpflicht** hinsichtlich der gesamten datenschutzrechtlichen Rechtslage des Staates der Datenverarbeitung nebst tatsächlicher Umsetzung. Dies bedeutet in der Praxis, dass der Auftraggeber als Verantwortlicher zwingend die datenschutzrechtliche Zulässigkeit der geplanten Leistung sowie die datenschutzrechtliche Zuverlässigkeit eines gegebenenfalls eingeschalteten (Unter-)Auftragsverarbeiters prüfen muss – wenn auch erst vor Aufnahme der Verarbeitung personenbezogener Daten und damit regelmäßig nicht bereits vor Zuschlagserteilung.[84] Aus praktischer Sicht sollte diese Prüfung allerdings so früh wie möglich erfolgen, um deren Ergebnis im besten Fall noch im laufenden Vergabeverfahren berücksichtigen zu können. Denn ist ein potenzieller (Unter-)Auftragnehmer erkennbar nicht in der Lage, seinen datenschutzrechtlichen Verpflichtungen während der Vertragsdurchführung auch tatsächlich zu entsprechen, so sind von ihm gegebenenfalls abgegebene anderslautende Erklärungen als nicht vorhanden anzusehen, was nach § 57 Abs. 1 Nr. 2 oder Nr. 4 VgV zum Ausschluss seines Angebots führt. Diese Prüfpflicht setzt sich in Form einer kontinuierlichen Überwachungspflicht des Auftraggebers als datenschutzrechtlich Verantwortlichem während der gesamten Auftragsausführung fort und umfasst in Bezug auf eventuelle Lösch- und/oder Aufbewahrungspflichten auch den nachvertraglichen Zeitraum. **71**

4. Dokumentation

Der Auftraggeber ist gemäß § 8 Abs. 1 Satz 1 VgV verpflichtet, das Vergabeverfahren von Beginn an fortlaufend in Textform nach § 126b Bürgerliches Gesetzbuch zu dokumentieren, soweit dies zur Begründung von Entscheidungen auf jeder Stufe des Vergabeverfahrens erforderlich ist. Die Dokumentation umfasst neben sämtlicher Kommunikation unter anderem die Vorbereitung der Auftragsbekanntmachung und der Vergabeunterlagen, die Öffnung der Angebote, Teilnahmeanträge und Interessensbestätigungen, die Verhandlungen und den Dialog mit den teilnehmenden Unternehmen sowie die Gründe für Auswahlentscheidungen und **72**

[83] OLG Karlsruhe, Beschluss vom 7. September 2022, 15 Verg 8/22, BeckRS 2022, 22588 m. w. N.

[84] Hartung, in: Kühling/Buchner, DSGVO/BDSG, 3. Aufl. 2020, Art. 28 Rn. 60; Gabel/Lutz, in: Taeger/Gabel, DSGVO/BDSG/TTDSG, 4. Aufl. 2022, Art. 28 Rn. 27, 31.

den Zuschlag, § 8 Abs. 1 Satz 2 VgV. § 8 Abs. 2 VgV statuiert dabei die Mindestanforderungen an den Vermerk. Sämtliche oben angeführten Fragestellungen und Erwägungen sind daher vom Auftraggeber schriftlich niederzulegen. Musterhafte Formblätter hierfür enthält beispielsweise das **Vergabehandbuch für Lieferungen und Leistungen Bayern**.[85]

73 Im Hinblick auf die datenschutzrechtlichen Fragestellungen ergibt sich eine **spezifische Dokumentationsverpflichtung aus Art. 5 Abs. 2 DSGVO** als Ausprägung der Rechenschaftspflicht. Diese setzt in Gestalt der erforderlichen Risikoanalyse für die Rechte und Freiheiten betroffener Personen bereits mit Ermittlung des Beschaffungsbedarfs, das heißt in der Vorbereitung der leistungsgegenständlichen Verarbeitung ganz zu Beginn des Vergabeverfahrens an. Betreffend die für den Datenschutz relevanten Aspekte kann die nach Art. 5 Abs. 2 DSGVO erforderliche Dokumentation auch für den Vergabevermerk nach § 8 VgV herangezogen werden.

[85] Fn. 7.

IV. Pflichten der Parteien nach Zuschlagserteilung

Die Pflichten der Parteien setzen sich nach Zuschlagserteilung entsprechend fort: So ist der **Auftraggeber** in der Ausführungsphase zur Kontrolle der Ordnungsmäßigkeit der Leistungserbringung verpflichtet; insbesondere hat er gemäß Art. 5 Abs. 2 DSGVO als datenschutzrechtlich Verantwortlicher für die Einhaltung der Anforderungen der Datenschutz-Grundverordnung zu sorgen. **74**

Der **bezuschlagte Bieter** muss seinerseits dafür Sorge tragen, dass er seine Leistung entsprechend den abgegebenen Garantien umsetzt und durchführt.[86] **75**

Für den Umgang mit nach Zuschlagserteilung veränderten Rahmenbedingungen und Änderungsverlangen müssen das geltende Vertragsrecht und insbesondere die Regelungen über die Zulässigkeit von Vertragsänderungen nach § 132 GWB beachtet werden. Entsprechende Vereinbarungen können auch in den Vertragsbedingungen getroffen werden; in den EVB-IT sind diese zum Teil bereits in den jeweiligen AGB enthalten.[87] **76**

[86] OLG Karlsruhe, Beschluss vom 7. September 2022, 15 Verg 8/22, BeckRS 2022, 22588.

[87] Vgl. z. B. Nr. 17 EVB-IT System AGB.

V. Nachprüfungsverfahren

77 Die Vergabe öffentlicher Aufträge oberhalb der gemäß § 106 GWB maßgeblichen Schwellenwerte unterliegt in Deutschland der Nachprüfung durch die Vergabekammern gemäß §§ 155 ff. GWB. Sie sind unabhängige Kontrollbehörden und in ihrer Organisation gerichtsähnlich, vgl. § 157 GWB. Fühlt sich ein Unternehmen, das an einer öffentlichen Ausschreibung teilgenommen hat, in seinen Rechten verletzt, so kann es gemäß § 160 GWB bei der Vergabekammer einen entsprechenden Antrag zur Prüfung stellen. Zwar gibt es nach § 163 Abs. 1 Satz 3 GWB im Nachprüfungsverfahren keine allgemeine Rechtmäßigkeitskontrolle; wird ein Nachprüfungsantrag jedoch für zulässig erachtet, prüft die Vergabekammer, ob ein nicht präkludierter[88] Verstoß gegen bieterschützende Vorschriften zu Lasten des Antragstellers vorliegt, und ergreift gegebenenfalls – ohne Bindung an Anträge, § 163 Abs. 1 Satz 1 und 2 in Verbindung mit § 168 Abs. 1 GWB – Maßnahmen, die im Interesse des Antragstellers zur Wiederherstellung eines fairen Wettbewerbs geeignet und notwendig sind. Ein Nachprüfungsantrag ist dann begründet, wenn nicht auszuschließen ist, dass es durch einen Verstoß gegen Vergabevorschriften zu einer Beeinträchtigung der Auftragschancen des Antragstellers gekommen ist.[89]

78 Die Prüfung der Vergabekammer im Rahmen eines Nachprüfungsverfahrens beschränkt sich ausweislich § 160 Abs. 2 Satz 1 in Verbindung mit § 97 Abs. 6 GWB auf Verstöße gegen das Vergaberecht. Datenschutzrechtliche Verstöße können vor der Vergabekammer daher nur dann geltend gemacht werden, wenn das Datenschutzrecht Anknüpfungspunkt einer vergaberechtlichen Brückennorm wie insbesondere des Gleichbehandlungsgrundsatzes ist:[90] Sofern ein Verstoß hiergegen gerügt wird und der öffentliche Auftraggeber diesen unter Verweis auf datenschutzrechtliche Anforderungen rechtfertigt, werden diese Gegenstand des Nachprüfungsverfahrens.

79 Unterhalb der EU-Schwellenwerte gibt es dagegen kein speziell vergaberechtliches Rechtsschutzverfahren, eventuell benachteiligte Mitbewerber sind auf die allgemeinen Rechtsschutzmöglichkeiten vor den Zivilgerichten verwiesen.[91] Diese umfassen insbesondere das allgemeine einstweilige Verfügungsverfahren der Zivilprozessordnung (bei ausnahmsweiser Kenntnis vor Zuschlagserteilung) sowie die Geltendmachung von Schadensersatzansprüchen – und im Ausnahmefall entgangenem Gewinn – bei vergaberechtswidrigen Entscheidungen des Auftraggebers (nach Zuschlagserteilung).

88 § 160 Abs. 3 GWB.

89 OLG Düsseldorf, Beschluss vom 8. März 2017, VII-Verg 39/16, BeckRS 2017, 106852; OLG Düsseldorf, Beschluss vom 28. Januar 2015, VII-Verg 31/14, BeckRS 2015, 9750; Dreher, in: Immenga/Mestmäcker, Wettbewerbsrecht, 6. Aufl. 2021, § 168 GWB Rn. 20.

90 OLG Düsseldorf, Beschluss vom 13. August 2008, VII-Verg 42/07, BeckRS 2008, 21712. Zum Beispiel eines gewerblichen Schutzrechts Dicks, in: Ziekow/Völlink, Vergaberecht, 4. Aufl. 2020, § 160 GWB Rn. 21.

91 BVerfG, Beschluss vom 13. Juni 2006, 1 BvR 1160/03.

VI. Rechtsfolgen bei Verstoß

Als Rechtsfolge eines Verstoßes gegen die Datenschutz-Grundverordnung drohen neben der soeben beschriebenen Abhilfe durch die Vergabekammer sowohl für den Auftraggeber als auch den (potenziellen) Auftragnehmer Untersagungsverfügungen der Aufsichtsbehörden nach Art. 58 Abs. 2 Buchst. f DSGVO, welche den Abbruch des Vergabeverfahrens zur Folge haben können. Für Bewerber oder Bieter kann die Missachtung datenschutzrechtlicher Vorschriften ferner, wie gesehen, eine „schwere Verfehlung" im Sinne des § 124 Abs. 1 Nr. 3 GWB darstellen, die einen fakultativen Ausschlussgrund begründet oder zum Ausschluss nach §§ 53 Abs. 7, 57 Abs. 1 Nr. 4 VgV führt. **80**

Darüber hinaus sind auch die allgemeinen Rechtsfolgen eines Schadensersatzanspruches einer von einer rechtswidrigen Datenverarbeitung betroffenen Person nach Art. 82 Abs. 1 DSGVO sowie eine Bußgeldbewehrung von Verstößen gegen die Datenschutz-Grundverordnung gemäß Art. 58 Abs. 2 Buchst. i in Verbindung mit Art. 83 DSGVO[92] zu beachten. Behörden und öffentliche Stellen sind von Bußgeldern allerdings weitgehend ausgenommen, Art. 83 Abs. 7 DSGVO in Verbindung mit Art. 22 Bayerisches Datenschutzgesetz. **81**

[92] Danach kann ein Verstoß gegen die Vorgaben der Datenschutz-Grundverordnung mit einem Bußgeld von bis zu 20 Millionen Euro oder 4 % des weltweiten Umsatzes des jeweiligen Verantwortlichen geahndet werden.

VII. Besondere Problemstellung: Beschaffung von Cloud-Services

82 Besonders komplex im Gefüge der Beschaffung datenschutzkonformer Leistungen stellen sich derzeit die Rechtmäßigkeitsvoraussetzungen der Vergabe von Cloud-Leistungen dar, wie die viel diskutierte Entscheidung der Vergabekammer Baden-Württemberg aus dem Sommer 2022 gezeigt hat.[93]

83 Cloud-Leistungen zeichnen sich dadurch aus, dass der Cloud-Anbieter einen Verbund von vielen Servern – die Cloud („Wolke") – zur Verfügung stellt, auf den seine Kunden über netzwerkfähige Geräte zugreifen, um eine bestimmte Leistung in Anspruch zu nehmen.[94] Dies hat zur Folge, dass die auf den Servern verarbeiteten Daten – jedenfalls für den Anwender – territorial nicht mehr „einem Server" und einem bestimmten geografischen Ort zugeordnet werden können; vielmehr können ihre Einzelbestandteile auf mehreren oder sogar allen Servern der Cloud verteilt sein. Zudem erfolgt die Verarbeitung der Daten in der Regel nicht durch den Kunden selbst, sondern durch den Anbieter der cloudbasierten Leistung als Auftragsverarbeiter. Diese Besonderheiten führen zu einer Vielzahl von rechtlichen Problemen und sind bereits im Rahmen der Leistungsbeschreibung und Vertragsgestaltung zu berücksichtigen: So geht die fehlende Lokalisierbarkeit der Daten mit einem Mangel an Transparenz einher, welcher seinerseits die Überprüfung der Datenschutzkonformität durch den Auftraggeber erschwert. Der Einsatz des Cloud-Anbieters als Auftragsverarbeiter im Sinne des Art. 28 DSGVO geht zusätzlich mit den oben bei Rn. 38 f. beschriebenen Implikationen einher.

1. Rechtsprechung

84 Grundlegend für die Beurteilung der datenschutzrechtlichen Rechtmäßigkeit von Cloud-Dienstleistungen ist dabei das Urteil des Europäischen Gerichtshofs vom 16. Juli 2020 in der Rechtssache „Schrems II".[95] Der Europäische Gerichtshof erklärte die bestehende Datenschutzvereinbarung der EU mit den USA („Privacy Shield") wegen Verstoßes gegen die Charta der Grundrechte der Europäischen Union und den Grundsatz der Verhältnismäßigkeit

[93] VK Baden-Württemberg, Beschluss vom 13. Juli 2022 , 1 VK 23/22, BeckRS 2022, 18405; aufgehoben durch OLG Karlsruhe, Beschluss vom 7. September 2022, 15 Verg 8/22, BeckRS 2022, 22588. Zu dieser Thematik beispielsweise auch BKartA, Beschluss vom 13. Februar 2023, VK 2-114/22, BeckRS 2023,2260.

[94] Die über eine Cloud angebotenen Leistungen können dabei in die Kategorien „Infrastructure as a Service" (Zugriff lediglich auf virtuelle Hardware, um eigene Betriebssysteme und Anwendungsprogramme zu nutzen), „Platform as a Service" (Nutzung virtueller Server, auf denen bereits ein Betriebssystem ausgeführt wird) und „Software as a Service" (Nutzung einer bestimmten Software) eingeteilt werden. Weiterhin wird typischerweise nach dem Nutzerkreis, also „Public Cloud", „Private Cloud" und „Hybrid Cloud", unterschieden. Zusammenfassend hierzu Claßen/Koch/Müller, Beschaffung von Cloud-Services durch öffentliche Auftraggeber, MMR 2020, 723, 724.

[95] C-311/18.

für ungültig (siehe Rn. 26). Ein Nachfolgemodell zu diesem Datenschutzabkommen wird frühestens Mitte 2023 in Kraft treten. Aus diesen Gründen existiert derzeit auch kein Angemessenheitsbeschluss im Sinne des Art. 45 Abs. 1 DSGVO für die USA. Schließlich ermöglichen auch die von der EU-Kommission vorabgenehmigten Standardvertragsklauseln wie gesehen in der Regel für sich genommen keine Datentransfers in die USA auf der Grundlage von Art. 46 DSGVO.

Gerade bei Leistungen betreffend die Verarbeitung personenbezogener Daten und insbesondere bei der Anwendung von Cloud-Lösungen mit dem Problem der Lokalisierbarkeit der Daten ist daher für öffentliche Auftraggeber die Beschränkung des Leistungsortes (siehe Rn. 25 ff.) auf die EU beziehungsweise den Europäischen Wirtschaftsraum (EWR) sowie auf Staaten, für die es einen Angemessenheitsbeschluss gibt, dringend anzuraten[96] und in Nr. 4 EVB-IT Cloud AGB sogar explizit geregelt.[97] **85**

Für die Konstellation, dass die Daten zwar in der EU beziehungsweise dem EWR verarbeitet werden, Anbieter der betreffenden Cloud allerdings eine Tochter eines US-amerikanischen Unternehmens ist,[98] besteht mit Blick auf den CLOUD Act sowie FISA 702 die abstrakte Gefahr einer nach EU-Recht unzulässigen Übermittlung von personenbezogenen Daten in einen Drittstaat. Denn beide Rechtsinstrumente beanspruchen Geltung über die Grenzen der USA hinaus: Der CLOUD Act (Clarifying Lawful Overseas Use of Data Act) ermöglicht US-Stellen grundsätzlich weitreichende Zugriffsbefugnisse, und zwar auch dann, wenn die Daten bei einem Tochterunternehmen in der EU liegen. Nach FISA 702 kann jeder „electronic communication service provider" zum Zwecke der (nachrichtendienstlichen) Überwachung von Nicht-US-Bürgern außerhalb des US-Territoriums zur Herausgabe von Daten verpflichtet werden.[99] **86**

An die gemäß Art. 28 Abs. 1, Erwägungsgrund 81 DSGVO erforderliche Prüfung der Zuverlässigkeit des Auftragsverarbeiters (und deren Dokumentation[100]) sind in diesem Fall nach einem Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder besonders hohe Anforderungen zu stellen, die dieser Gefahr Rechnung tragen.[101] Zur Sicherstellung eines angemessenen Datenschutzniveaus sind insbesondere **87**

96 Zumindest inzident anerkannt in den Entscheidungen der VK Baden-Württemberg, Beschluss vom 13. Juli 2022, 1 VK 23/22, BeckRS 2022, 18405, und des OLG Karlsruhe, Beschluss vom 7. September 2022, 15 Verg 8/22, BeckRS 2022, 22588. Siehe auch VK Südbayern, Beschluss vom 8. Februar 2023, 3194-Z3-3_01-22-42, IBRRS 2023, 0880.

97 Nach Nr. 4 EVB-IT Cloud hat die Speicherung und sonstige Verarbeitung von Daten des Auftraggebers durch den Auftragnehmer ausschließlich innerhalb der EU und des EWR zu erfolgen sowie, sofern ein Angemessenheitsbeschluss gemäß Art 45 DSGVO besteht, in der Schweiz. Eine Ausnahme greift nur dann, wenn der Auftraggeber in der Administrationskonsole zusätzlich weitere Regionen für die Leistung ausgewählt hat.

98 Vgl. für einen entsprechenden Sachverhalt VK Baden-Württemberg, Beschluss vom 13. Juli 2022, 1 VK 23/22, BeckRS 2022, 18405.

99 Dies umfasst nicht nur klassische Telekommunikationsunternehmen, sondern auch Anbieter von elektronischen Kommunikationsdiensten („electronic communication services"), Anbieter von Computerspeicher- und Verarbeitungsleistungen („remote computing„services"), Anbieter sonstiger Kommunikationsdienste mit Zugriffsmöglichkeiten sowie Mitarbeiter und Vertreter bzw. Beauftragte solcher Unternehmen. Letzteres umfasst auch Tochtergesellschaften.

100 VK Südbayern, Beschluss vom 8. Februar 2023, 3194-Z3-3_01-22-42, IBRRS 2023, 0880.

101 DSK, Zur datenschutzrechtlichen Bewertung von Zugriffsmöglichkeiten öffentlicher Stellen von Drittländern

technische und organisatorische Maßnahmen zu ergreifen, die die Einhaltung der Datenschutz-Grundverordnung hinreichend garantieren. Konkret bedeutet dies, dass die Maßnahmen sicher verhindern müssen, dass das Tochterunternehmen Herausgabeanordnungen auf der Basis der o. a. Rechtsnormen erfüllt.[102] In Betracht kommen insbesondere eine Verschlüsselung und/oder Pseudonymisierung der Daten oder vergleichbare technisch-organisatorische Maßnahmen, die einen Zugriff faktisch ausschließen,[103] wobei zu beachten ist, dass der Europäische Datenschutzausschuss für den Fall, dass der Empfänger leistungsartbedingt personenbezogene Daten im Klartext verarbeiten muss, keine ergänzenden Schutzmaßnahmen identifizieren konnte, die zu einer Rechtmäßigkeit des Datenexports führen könnten.[104] Sollte der Verantwortliche nach dieser Prüfung zu der Bewertung kommen, dass der Auftragsverarbeiter keine hinreichenden Garantien gemäß Art. 28 Abs. 1 DSGVO bietet, muss er selbst technische und organisatorische Maßnahmen ergreifen, um die festgestellten Defizite auszugleichen und so die Risiken einer unzulässigen Drittlandsübermittlung zu vermeiden. Die Umsetzung und Einhaltung sämtlicher Maßnahmen muss der Auftraggeber nach Zuschlagserteilung in der Ausführungsphase kontrollieren. Dies gestaltet sich bei Cloud-basierten Leistungen durchaus komplex.

2. Einzelaspekte

88 Nicht nur mit Blick auf die fehlende Lokalisierbarkeit der Daten und die damit verbundenen Problemstellungen stellt die Beschaffung von Cloud-Leistungen eine besondere Herausforderung dar. Auch auf Grund der vernetzten, lokal nicht eingrenzbaren, extrem arbeitsteiligen Prozesse sowie der regelmäßigen Einordnung als Auftragsverarbeitung im Sinne des Art. 28 DSGVO weist die Vergabe von Cloud-Services Besonderheiten auf. Aufgrund ihrer hohen

auf personenbezogene Daten, Beschluss vom 31. Januar 2023, Internet: https://www.datenschutzkonferenz-online.de/beschluesse-dsk.htm. Zum Umfang der Prüfpflicht des Auftraggebers betreffend technisch-organisatorische Maßnahmen bei Cloud-Leistungen vgl. VK Südbayern, Beschluss vom 8. Februar 2023, 3194-Z3-3_01-22-42, IBRRS 2023, 0880.

102 Zu möglichen Maßnahmen vgl. Europäischer Datenschutzausschuss, Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten, Stand 7/2021, Rn. 75.

103 Conseil d'Etat, Beschluss vom 12. März 2021, 450163 – „Doctolib", Internet: https://www.legifrance.gouv.fr/ceta/id/CETATEXT000043261200. – Vgl. auch Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg, Stellungnahme zum Beschluss der Vergabekammer Baden-Württemberg vom 13.07.2022 (Az. 1 VK 23/22), S. 2, Internet: https://www.baden-wuerttemberg.datenschutz.de/stellungnahme-zum-beschluss-der-vergabekammer-bw. Im konkreten Fall von der Nachprüfungsinstanz OLG Karlsruhe, Beschluss vom 7. September 2022, 15 Verg 8/22, BeckRS 2022, 22588, nicht einzelfallbezogen geprüft. Weniger restriktiv die dänische Datenschutzbehörde, die in ihren Leitlinien zu Cloud-Diensteanbietern (CSP) „Guidance on the use of cloud", März 2022, Internet: https://www.datatilsynet.dk/Media/637824108733754794/Guidance%20on%20the%20use%20of%20cloud.pdf, ausführt: „Lastly, even if the specific data you wish to transfer effectively falls within in the scope of the surveillance programme authorised under inter alia FISA 702, you may still – without taking any additional action – transfer personal data to your CPS. This presupposes, however, that your supplier, in practice has not received any requests from US law enforcement authorities in the past, or that the types of personal data that you intend to transfer have not in any case fallen within the scope of such requests" (S. 25).

104 Anhang 2 Anwendungsfall 6 der Empfehlungen 01/2020, siehe Fn. 99.

Verfügbarkeit und Skalierbarkeit sowie der häufig niedrigeren Kosten, Betriebsaufwände und Know-how-Anforderungen kommt Cloud-Technologien aber eine zunehmende Bedeutung zu.[105]

Diese Umstände und Unsicherheiten können durch die Nutzung sog. **Sovereign Clouds** zumindest verringert werden. Diese souveränen Clouds sind durch autarke Konzeptionierung oder auch Open Source Lösungen gekennzeichnet. Im Gegensatz zur konventionellen Cloud sind Sovereign Clouds durch besondere Maßnahmen geschützt, die eine höhere Datensicherheit gewährleisten und einen Fremdzugriff ausschließen sollen.[106] So bietet beispielsweise das staatliche Rechenzentrum des Freistaates Bayern mit der „BayernBox" und der „SecureBox Bayern" eigene Cloud-Lösungen an, welche von der Staatsverwaltung grundsätzlich genutzt werden müssen.[107] 89

Sollte der Auftraggeber eine konventionelle Cloud nutzen (müssen), können neben den vom Bundesamt für Sicherheit in der Informationstechnik aufgestellten „**Requirements for Cloud Platforms in the Federal Administration**"[108] und dem Leitfaden „Cloud Computing" des Landesamts für Sicherheit in der Informationstechnik (BSI)[109] die neuen **EVB-IT Cloud** eine Orientierungshilfe darstellen.[110] Letztere zählen zu den Basisverträgen und erfassen inhaltlich die Beschaffung von Cloud-Leistungen, insbesondere Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) sowie Managed Cloud Services (MCS). Es steht sogar ein spezifischer Kriterienkatalog für Cloud-Leistungen zur Verfügung. Beim Datenschutz und der IT-Sicherheit orientieren sich die EVB-IT Cloud dabei am C5 Kriterienkatalog (Cloud Computing Compliance Criteria Catalogue) des Bundesamts für Sicherheit in der Informationstechnik, vgl. Nr. 1.2 EVB-IT Cloud AGB. Weitergehende Regelungen zu den zentralen Themen Datenschutz, IT-Sicherheit und Vertraulichkeit finden sich in Nr. 4 und 6 der EVB-IT Cloud AGB. Insoweit ist allerdings in jedem Einzelfall zu prüfen, ob die in den 90

[105] S. auch Digitalstrategie der Bundesregierung, Internet: https://www.bundesregierung.de/breg-de/themen/digitaler-aufbruch/datenstrategie-2001284.

[106] Zum Ganzen Rath/Keller, US Cloud-Anbieter, der „Risikofaktor US CLOUD Act", das Vergaberecht und die Nachfrage nach sicheren Sovereign Clouds, CR 2022, 682, 685 ff. Die Sovereign Cloud ist dabei als „überwachte Cloud" (Treuhänder-Modell, das einen Zugriff auf Daten nicht verhindern kann), „Hosted Cloud" bzw. „on Premise Cloud" (Betrieb der Cloud auf eigener Hardware in eigenen Rechenzentren und gegebenenfalls am Standort des Auftraggebers) oder als „Confidential Computing" (Isolierung der Daten in einer gesicherten „Enklave") denkbar.

[107] Landesamt für Sicherheit in der Informationstechnik, IT-Sicherheitsleitfaden für Behörden und öffentliche Unternehmen im Freistaat Bayern, Einsatz von Diensten und Produkten mit Cloud-Technologien, Stand 7/2020, S. 8, 12 f., Internet: https://lsi.bybn.de/ikt/index.php (nur über das Bayerische Behördennetz abrufbar).

[108] 17. Juni 2022, Internet: https://fragdenstaat.de/anfrage/rote-linien-des-bsi-fuer-cloud-angebote-fuer-die-oeff-verwaltung/707433/anhang/cloud-platform-requirements.pdf

[109] Landesamt für Sicherheit in der Informationstechnik (Fn. 107). Zu beachten gilt, dass beim Einsatz externer Services aus Sicht des zentralen IT-Controllings eine Vorhabensanzeige und Genehmigung notwendig ist, S. 8.

[110] Die EVB-IT Cloud stehen seit 1. März 2022 zur Verfügung. Neben dem EVB-IT Cloud Vertrag und den EVB-IT Cloud AGB gibt es mit dem EVB-IT Cloud Kriterienkatalog für Cloudleistungen und den EVB-IT Cloud Anlage auftragnehmerseitige AGB zwei weitere Vorlagen zur optionalen Verwendung sowie Hinweise für die Nutzung der Dokumente. Die EVB-IT Cloud werden 18 Monate nach ihrer Veröffentlichung einer erneuten Prüfung unterzogen und – sofern erforderlich – angepasst werden.

EVB-IT Cloud enthaltenen Standards ausreichend oder ob weitergehende Regelungen erforderlich sind. Insbesondere für Kritische Infrastrukturen oder sonstige Konstellationen mit besonderer Sensibilität bedarf es gegebenenfalls ergänzender Bestimmungen.

91 **Zertifikate und Testate** speziell für Clouds sind beispielsweise das Gütesiegel Euro-Cloud Star Audit von EuroCloud, CSA Star der Cloud Security Alliance, Certified Cloud Service vom TÜV Rheinland, ISO 27001 sowie der Cloud Computing Compliance Criteria Catalogue und das IT-Grundschutz-Zertifikat des BSI.

92 Noch **vor Inkrafttreten der Datenschutz-Grundverordnung** datieren die „Orientierungshilfe – Cloud Computing" der deutschen Aufsichtsbehörden,[111] das „Sopot Memorandum"[112] sowie die Stellungnahme der Art. 29-Datenschutzgruppe zur datenschutzgerechten Nutzung von Cloud-Computing.[113]

93 Noch in der Umsetzung befindet sich die im Jahr 2021 beschlossene **Verwaltungs-Cloud-Strategie des IT-Planungsrates**, die mithilfe von Multi-Cloud-Strukturen auf eine Reduktion der Abhängigkeit von einzelnen Anbietern und Produkten zielt.[114]

[111] Orientierungshilfe – Cloud Computing der Arbeitskreise Technik und Medien der DSK sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises, Stand 10/2014.

[112] International Working Group on Data Protection in Telecommunications, 675.44.10, Arbeitspapier Cloud Computing – Fragen des Schutzes der Privatsphäre und des Datenschutzes – „Sopot Memorandum", 51. Sitzung, 23.–24. April, Sopot (Polen), Internet: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Berlin-Group/20120424_AP_Sopot-Memorandum.html.

[113] Artikel-29-Datenschutzgruppe, Stellungnahme 05/2012 zum Cloud Computing, Stand 7/2012, 01037/12/DE, WP 196.

[114] Vgl. https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-46_Deutsche_Verwaltungscloud_Strategie_AL1.pdf.

VIII. Fazit

Die Durchführung ordnungsgemäßer Vergabeverfahren für datenschutzkonforme Leistungen ist zwar durchaus komplex und insbesondere im Zusammenhang mit der Bestimmung des Beschaffungsbedarfs mit hohen Anforderungen verbunden. Gleichzeitig bietet das Vergaberecht aber auch zahlreiche Ansatzpunkte und Gestaltungsmöglichkeiten für datenschutzrechtliche Vorgaben an die nachgefragte Leistung – ein Potenzial, das von öffentlichen Auftraggebern genutzt werden sollte. **94**

Das Verhandlungsverfahren mit Teilnahmewettbewerb gewährt insoweit die größten Verhandlungsmöglichkeiten, während der wettbewerbliche Dialog einen recht weitgehenden Gestaltungsspielraum eröffnet. Um Fehler – nicht nur in datenschutzrechtlicher Sicht, sondern ganz generell – möglichst zu vermeiden, empfiehlt sich die Nutzung der vorhandenen Muster und Formularblätter, insbesondere in Gestalt der EVB-IT sowie der Vorlagen aus dem Vergabehandbuch für Lieferungen und Leistungen Bayern.[115] **95**

Die nachfolgende Tabelle enthält zusammenfassend mögliche Ansatzpunkte für die Gewährleistung der Datenschutzkonformität zu beschaffender Liefer- oder Dienstleistungen im Verlauf eines Vergabeverfahrens: **96**

[115] VHL Bayern, Fn. 7.