Kommentar zur Änderung des Referentenentwurfs zum Vergabebeschleunigungsgesetz in der Version des Kabinettsentwurfs vom 06.08.2025

Einleitung/Allgemeines

Wir begrüßen die Möglichkeit, zum Vergabebeschleunigungsgesetz in der letzten Fassung des Kabinettentwurfs Stellung zu nehmen.

Wir haben gesehen, dass bereits die Frist zur Abgabe von Stellungnahmen im Rahmen der Konsultation zum Referentenentwurf sehr kurz bemessen war. Die Bundesregierung hat sich im Koalitionsvertrag verpflichtet, ausreichend Zeit für die Beteiligung einzuräumen. Da dies hier nicht der Fall war, besteht aus unserer Sicht die Gefahr, dass ein so enger Zeitrahmen eine **gründliche Prüfung und konstruktive Rückmeldung von Unternehmen und Verbänden** maßgeblich erschwert.

Angesichts der weitreichenden Kompetenzerweiterungen des Gesetzesentwurfs und ihrer potentiellen Auswirkungen auf Fragen der Innovationsfähigkeit, Zukunftsfähigkeit und Wettbewerbsfähigkeit **sollte Verbänden und Wirtschaftsvertretern und weitere Gelegenheit zur Stellungnahme gegeben werden**.

Digitale Angebote und informationstechnische Systeme spielen eine wachsende Bedeutung im gesamten wirtschaftlichen und gesellschaftlichen Spektrum. Mit der dadurch zunehmenden (hybriden) Bedrohungslage ist es grundsätzlich zu **begrüßen, dass die Bundesregierung bei der öffentlichen Beschaffung verstärkt auf beschleunigte Beschaffungspraktiken setzt**. Dies wirft jedoch unmittelbar wichtige Folgefragen auf, die der Gesetzgeber bisher unbeantwortet gelassen hat.

Die Auswahl geeigneter Maßnahmen kann nur auf Basis eines klaren Zielverständnisses erfolgen. Alle Maßnahmen müssen hinsichtlich ihrer Innovationsfreundlichkeit, ihres Investitionsschutzes und ihrer Rechtssicherheit überprüft und bewertet werden. Grundvoraussetzung für die Gewährleistung eines hohen Cybersicherheitsniveaus ist, dass alle relevanten Akteure – von Unternehmen bis hin zu Behörden – vertrauensvoll und kooperativ zusammenarbeiten und ihre jeweilige Verantwortung im Gesamtökosystem wahrnehmen.

Dies erfordert einen **fairen Wettbewerb, der grundsätzliche Gleichbehandlung** vorsieht und **Innovationen fördert**. Ein **technologieneutraler Ansatz** ist dabei von grundlegender Bedeutung. Für alle Hersteller sollten dieselben produkt- und dienstleistungsspezifischen Prüfkriterien, Regeln und Verfahren gelten, unabhängig von ihren Produkten und Dienstleistungen sowie ihrer Herkunft. Die Zusammenarbeit darf nicht auf die nationale Ebene beschränkt bleiben. Auf EU-Ebene **existiert außerdem bereits ein entsprechender Rahmen für Cybersicherheit und Resilienz** (DORA, NIS2, CER bzw. nationale Umsetzungsvorschriften). Dabei handelt es sich um bestehende Sicherheitsanforderungen für die öffentliche Auftragsvergabe.

Gerade vor dem Hintergrund der intendierten Steuerungswirkung führt die **Einführung einer nationalen Anforderung zu digitaler Souveränität zum genauen Gegenteil einer beschleunigten Auftragsvergabe**. Es wird vielmehr eine neue Hürde geschaffen, die zusätzliche Prüfungen, Kriterien und Unsicherheiten mit sich bringt und somit das Vergabeverfahren verlängert, insbesondere angesichts der nicht klar definierten Anforderungen, wie sie dem neu eingeführten Einschub und dessen Begründung zu entnehmen sein sollen. Außerdem kann die geschaffene Einengung **ungewollt dazu führen, bestehende Abhängigkeiten eher weiter zu verstärken**.

Zusätzlich besteht eine nicht unerhebliche Gefahr, dass mit der Einführung bestimmter Definitionsmerkmale für “digitale Souveränität” durch den vorliegenden Entwurf **unbeabsichtigte und gegenläufige Folgewirkungen in anderen Bereichen der im Koalitionsvertrag dazu adressierten Themenfelder entstehen**.

Der Verweis auf die zusätzliche Anforderung der „digitalen Souveränität“ sollte daher aus dem Entwurf des § 128 Abs. 2 GWB ersatzlos gestrichen werden. Die Ergänzung ist überschießend, läuft dem Ziel des Gesetzes entgegen und ist aus unserer Sicht mit geltendem Recht nicht vereinbar.

Im Einzelnen:

Begriffliche Unschärfe und Überschießende Tendenz

Der sehr weite Auslegungsrahmen des unbestimmten Begriffs „digitale Souveränität“ im Zusammenhang mit „Versorgungssicherheit“ erschwert die Beurteilung dieses Standards, ohne dass weitere Details oder Verweise gewährt werden. Der Begriff „digitale Souveränität“ gewinnt in aktuellen politischen Debatten an Bedeutung, eine **rechtlich eingefasste Definition ist jedoch nicht ohne Grund bislang bewusst unterblieben**. Er wird unterschiedlich interpretiert, beinahe inflationär verwendet und ist nicht operationalisiert.

Selbst wenn dies eine strategische Unklarheit seitens des Gesetzgebers wäre, kann die Verwendung vager Begriffe seitens der Betreiber zu zusätzlicher Unsicherheit in Vergabeprozessen führen und sich somit disruptiv auf die digitale Wirtschaft und andere kritische Infrastruktursektoren auswirken. Die aktuell gewählte Formulierung wirft hier zahlreiche zentrale Fragen auf: **Wann gelten Anbieter und/oder die Nutzung von Komponenten als sicher „digital souverän“** (und gegebenenfalls im Einklang mit den sicherheitspolitischen Zielen der Bundesrepublik Deutschland, der Europäischen Union oder des NATO-Vertrages)?

Zu beachten ist zudem, dass die aktuellen Bemühungen, Sicherheit und Souveränität zusammen zu regeln, mit einem zunehmenden bürokratischen Aufwand einhergehen. Es gibt derzeit keinen einheitlichen Kriterienkatalog innerhalb der Bundesregierung, der regelt, wie stark bestimmte Anforderungen bei der Vergabe öffentlicher Aufträge für souveräne Cloud-Dienste gewichtet werden sollen. Einer Antwort auf eine parlamentarische Anfrage (Drucksache 20/15138; https://dserver.bundestag.de/btd/20/151/2015138.pdf; Antw. der BReg auf Fragen der Kleinen Anfrage, Fragenr. 3-3o.) zufolge wurden kürzlich in einer **ressortübergreifenden Umfrage mindestens 15 Bewertungskriterien vorgeschlagen**, wobei die verschiedenen Bundesministerien teilweise sehr unterschiedliche Einschätzungen vorgenommen haben.

Bereits die Diskussion über zusätzliche Souveränitätsanforderungen auf EU-Ebene im **technischen Kontext der EUCS-Zertifizierung hat viele unterschiedliche Perspektiven der Regulierungsbehörden** in den verschiedenen Mitgliedstaaten aufgezeigt, wie souveräne Interessen in Marktanforderungen umgesetzt werden sollten. Bis heute gibt es kein einheitliches Verständnis von digitaler Souveränität und ihrer Umsetzung im Rahmen verschiedener Marktsektoren (strategische Anwendungsfälle).
Versorgungssicherheit ist ursprünglich auf physische Güter (z. B. Medikamente) ausgerichtet; ihre Übertragung auf digitale Angebote ist unklar und könnte willkürliche Eingriffe rechtfertigen.

Verbindung zum Auftragsgegenstand und Gleichbehandlung

Die Einführung von Vergabebeschränkungen auf Basis eines Kriteriums „Belange der Digitalen Souveränität“ birgt erhebliche rechtliche Risiken, da es die grundlegenden Prinzipien des Vergaberechts, insbesondere die **Verbindung zum Auftragsgegenstand**, untergräbt. Gemäß § 127 Abs. 3 S.1 GWB müssen alle Zuschlagskriterien in einem direkten **Zusammenhang mit der konkreten zu erbringenden Leistung** stehen. Kriterien wie die Lokalisierung von Daten, spezifische Personalanforderungen oder die „rechtliche, organisatorische und technische Immunität gegen unerwünschte Zugriffe“ sind jedoch nicht unmittelbar an den Leistungsgegenstand gebunden. Sie **beschreiben nicht die spezifische Qualität, den Herstellungsprozess oder die Merkmale der zu liefernden Dienstleistung oder Ware**, sondern die allgemeine Aufstellung des bietenden

Unternehmens. Ein Kriterium wie die Lokalisierung von Daten beschreibt ebenfalls nicht das Produkt selbst oder ist konkret genug, sondern Rahmenbedingungen, unter denen ein Unternehmen operiert. § 127 Abs. 3 S. 1 GWB ist aber gerade dazu gedacht, zu verhindern, dass strukturpolitisch erwünschte Aspekte ohne direkten Konnex ungefiltert in das Vergaberecht einfließen (s. z.B. Lausen/Pustal: Berücksichtigung von Nachhaltigkeitskriterien im Vergabeverfahren, NZBau 2022, 3)

Dies würde darüber hinaus eine **unzulässige Einzelfallregulierung** darstellen, da sie bestimmte Anbieterstrukturen bevorzugt oder ausschließt, ohne dass dies durch die spezifischen Anforderungen des Auftrags sachlich gerechtfertigt wäre. Dies verstößt gegen das Diskriminierungsverbot und den Gleichbehandlungsgrundsatz und würde ohne klare Kriterien zu einer unzulässigen Beschränkung des Wettbewerbs führen.

Soweit überhaupt eine Definition von “digitaler Souveränität“ und „Versorgungssicherheit“ gewollt ist, müsste diese mit **messbaren, nachvollziehbaren Kriterien versehen sein**. EIne Definition muss auf bestimmte, klar definierte Bereiche (z. B. kritische Infrastruktur, Verteidigung, Arzneimittelversorgung) beschränkt werden, auch um Widersprüche oder Inkompatibilitäten mit bereits geltenden Rechtsvorschriften auszuschließen.

Transparenz und Rechenschaftspflichten

Die Einführung von Kriterien zur digitalen Souveränität müsste außerdem **Transparenz- und Rechenschaftspflichten** einbeziehen. Um eine rechtliche Grauzone zu vermeiden, müsste die Anwendung solcher Kriterien durch Berichts-, Dokumentations- und Überprüfungspflichten nachvollziehbar gemacht werden. Zudem bedarf es dann einer **obligatorischen Gesetzesfolgenabschätzung**, die die Auswirkungen auf Wettbewerb, Innovation und Marktstruktur untersucht und in einem entsprechenden Gesetzesentwurf reflektiert ist.

Die Anwendung sollte, wenn überhaupt, **auf Ausnahmefälle beschränkt bleiben**, etwa mit einer Notfallklausel mit klaren Überprüfungskriterien in Krisen- oder Sicherheitslagen, um den Grundsatz der Verhältnismäßigkeit zu wahren und eine übermäßige Einschränkung des Wettbewerbs zu verhindern.

Soweit mit dem Einschub eine etwaige Benachteiligung von Open-Source-Cloud-Anbietern adressiert werden soll, halten wir die Schaffung zusätzlicher rechtlich verbindlicher Quoten in der öffentlichen Beschaffung nicht für notwendig: Voraussetzung ist, dass entsprechende Lösungen am Markt verfügbar sind und die Anbieter Betrieb und Wartung zuverlässig gewährleisten können. Vor dem Hintergrund des kürzlich im E-Government-Gesetz (§ 16a EGovG) verankerten Vorrangs für Open Source-Software geht die Bundesregierung daher davon aus, dass ihr Anteil in der Bundesverwaltung künftig weiter steigen wird. Weiterer Handlungsbedarf besteht auch aus diesem Grunde aus unserer Sicht nicht.

Gesetz gegen Wettbewerbsbeschränkungen (GWB) (aktuell)

§ 127 Zuschlag
(1) Der Zuschlag wird auf das wirtschaftlichste Angebot erteilt. Grundlage dafür ist eine Bewertung des öffentlichen Auftraggebers, ob und inwieweit das Angebot die vorgegebenen Zuschlagskriterien erfüllt. Das wirtschaftlichste Angebot bestimmt sich nach dem besten Preis-Leistungs-Verhältnis. Zu dessen Ermittlung können neben dem Preis oder den Kosten auch qualitative, umweltbezogene oder soziale Aspekte berücksichtigt werden.
(2) Verbindliche Vorschriften zur Preisgestaltung sind bei der Ermittlung des wirtschaftlichsten Angebots zu beachten.
(3) Die Zuschlagskriterien müssen mit dem Auftragsgegenstand in Verbindung stehen. Diese Verbindung ist auch dann anzunehmen, wenn sich ein Zuschlagskriterium auf Prozesse im Zusammenhang mit der Herstellung, Bereitstellung oder Entsorgung der Leistung, auf den Handel mit

der Leistung oder auf ein anderes Stadium im Lebenszyklus der Leistung bezieht, auch wenn sich diese Faktoren nicht auf die materiellen Eigenschaften des Auftragsgegenstandes auswirken.
(4) Die Zuschlagskriterien müssen so festgelegt und bestimmt sein, dass die Möglichkeit eines wirksamen Wettbewerbs gewährleistet wird, der Zuschlag nicht willkürlich erteilt werden kann und eine wirksame Überprüfung möglich ist, ob und inwieweit die Angebote die Zuschlagskriterien erfüllen. Lassen öffentliche Auftraggeber Nebenangebote zu, legen sie die Zuschlagskriterien so fest, dass sie sowohl auf Hauptangebote als auch auf Nebenangebote anwendbar sind.
(5) Die Zuschlagskriterien und deren Gewichtung müssen in der Auftragsbekanntmachung oder den Vergabeunterlagen aufgeführt werden.

§ 128 Auftragsausführung
(1) Unternehmen haben bei der Ausführung des öffentlichen Auftrags alle für sie geltenden rechtlichen Verpflichtungen einzuhalten, insbesondere Steuern, Abgaben und Beiträge zur Sozialversicherung zu entrichten, die arbeitsschutzrechtlichen Regelungen einzuhalten und den Arbeitnehmerinnen und Arbeitnehmern wenigstens diejenigen Mindestarbeitsbedingungen einschließlich des Mindestentgelts zu gewähren, die nach dem Mindestlohngesetz, einem nach dem Tarifvertragsgesetz mit den Wirkungen des Arbeitnehmer-Entsendegesetzes für allgemein verbindlich erklärten Tarifvertrag oder einer nach § 7, § 7a oder § 11 des Arbeitnehmer-Entsendegesetzes oder einer nach § 3a des Arbeitnehmerüberlassungsgesetzes erlassenen Rechtsverordnung für die betreffende Leistung verbindlich vorgegeben werden.
(2) Öffentliche Auftraggeber können darüber hinaus besondere Bedingungen für die Ausführung eines Auftrags (Ausführungsbedingungen) festlegen, sofern diese mit dem Auftragsgegenstand entsprechend § 127 Absatz 3 in Verbindung stehen. Die Ausführungsbedingungen müssen sich aus der Auftragsbekanntmachung oder den Vergabeunterlagen ergeben. Sie können insbesondere wirtschaftliche, innovationsbezogene, umweltbezogene, soziale oder beschäftigungspolitische Belange oder den Schutz der Vertraulichkeit von Informationen umfassen.

Kabinettsversion neu

15. § 128 wird wie folgt geändert:
a) […

b) In Absatz 2 wird nach der Angabe „Belange“ die Angabe „Belange der Versorgungssicherheit **oder der digitalen Souveränität“** eingefügt.

Zu Nummer 15 (§128 GWB), S. 66
Zu Buchstabe b

Mit Blick auf die in § 128 Absatz 2 geregelten besonderen Ausführungsbedingungen wird durch die Einfügung der Wörter „Belange der Versorgungssicherheit“ klargestellt, dass insoweit – etwa zwecks Reduzierung strategischer Abhängigkeiten – auch entsprechende Belange Berücksichtigung finden können, beispielweise durch Vorgaben an den Produktionsstandort in Bereichen wie etwa der Versorgung der Bevölkerung mit kritischen Arzneimitteln. Gleiches gilt für Belange der digitalen Souveränität. Diese Belange können beispielsweise berücksichtigt werden durch Anforderungen an die Nutzung interoperabler und offener IT-Systeme oder Software, die Nachvollziehbarkeit und Kontrolle von Datenverarbeitungsvorgängen, besondere Anforderungen an das im Rahmen der Datenverarbeitung eingesetzte Personal, Anforderung an Sicherheitsvorkehrungen, die Lokalisierung von Daten sowie die rechtliche, organisatorische und technische Immunität gegen unerwünschte Zugriffe oder Verfügbarkeitseinschränkungen. Ziel ist es, die Kontrolle über digitale Infrastrukturen, Datenverarbeitung und informationstechnische Systeme im Rahmen öffentlicher Aufträge zu stärken und Abhängigkeiten von Anbietern zu reduzieren.