abzusehen.[97] Von diesen Regelungen profitieren zudem die Auftragnehmer, die bei der Vergabe von Unteraufträgen nach den gleichen Maßstäben zu verfahren haben.[98]

b) Keine zwingende Unwirksamkeit des Auftrags bei einem Verstoß gegen § 135 GWB

Nicht jeder Verstoß des Auftraggebers gegen § 135 GWB führt zur Unwirksamkeit des öffentlichen Auftrags. Ein Vertrag kann auf Antrag des Auftraggebers als nicht unwirksam erachtet werden,

> „wenn nach Prüfung aller maßgeblichen Gesichtspunkte unter Berücksichtigung des Zweckes i.S.d. § 1 der besonderen Verteidigungs- und Sicherheitsinteressen sowie der unmittelbaren Stärkung der Einsatzfähigkeit der Bundeswehr zwingende Gründe eines Allgemeininteresses es ausnahmsweise rechtfertigen, die Wirkung des Vertrages zu erhalten."[99]

Die Nachprüfungsinstanzen erlassen in diesen Fällen alternative Sanktionen zur Feststellung der Unwirksamkeit, die wirksam, verhältnismäßig und abschreckend sind. Sie umfassen die Verhängung einer Geldsanktion gegen den Auftraggeber von höchstens 15 Prozent des Auftragswertes oder die Verkürzung der Laufzeit des Vertrages.[100] Es ist allerdings fraglich, ob eine Geldsanktion von höchstens 15 Prozent des Auftragswertes eine für den Auftraggeber abschreckende Sanktion darstellt, die ihn von einem Verstoß gegen § 135 GWB abhält.

c) Beschränkung des Vergabeverfahrens auf europäische Bewerber und Bieter

Der Auftraggeber darf die Teilnahme an einem Vergabeverfahren auf Bewerber oder Bieter beschränken, die in einem Mitgliedstaat der Europäischen Union ansässig sind, wenn der öffentliche Auftrag im Rahmen eines Kooperationsprogramms vergeben wird, welches mit mindestens einem anderen Mitgliedstaat der Europäischen Union durchgeführt wird.[101]

Bewerber oder Bieter, die in einem Staat außerhalb der Europäischen Union ansässig sind, der nicht die notwendige Gewähr für die Wahrung der Sicherheitsinteressen der Bundesrepublik Deutschland bietet, darf der Auftraggeber ausschließen.[102] Der Auftraggeber darf weiterhin von den Bietern verlangen, in ihrem Angebot keine Unterauftragnehmer vorzusehen und zu beauftragen, die in einem Staat außerhalb der Europäischen Union ansässig sind, der nicht die notwendige Gewähr für die Wahrung der Sicherheitsinteressen der Bundesrepublik Deutschland bietet.[103]

Diese Beschränkungen gelten jedoch nicht in Bezug auf solche Bewerber, Bieter, Auftragnehmer und Unterauftragnehmer, die in einem Staat ansässig sind, der Vertragspartei des Abkommens über den Europäischen Wirtschaftsraum (»EWR«) ist oder der dem Übereinkommen über das öffentliche Beschaffungswesen von 1994 (»GPA«) oder anderen, für die Europäische Union bindenden internationalen Übereinkommen beigetreten ist, wenn der öffentliche Auftrag in den Anwendungsbereich des jeweiligen Übereinkommens fällt.[104]

d) Vereinfachte Beschaffung im Rahmen eines Kooperationsprogramms

Dem Auftraggeber stehen gem. § 4 Abs. 2 BwBBG weitere Erleichterungen bei der Auftragsvergabe zur Verfügung, wenn ein öffentlicher Auftrag gem. § 104 GWB im Rahmen eines Kooperationsprogramms, welches mit mindestens einem anderen Mitgliedstaat der Europäischen Union durchgeführt wird, oder auf andere Weise gemeinsam mit einem anderen Mitgliedstaat der Europäischen Union oder mit der Europäischen Union vergeben wird, und dieser öffentliche Auftrag in den Anwendungsbereich des Teils 4 des GWB fällt.

e) Beschleunigung von Nachprüfungsverfahren

Eine Beschleunigung von Nachprüfungsverfahren soll mit dem BwBBG dadurch erreicht werden, dass mündliche Verhandlungen im Wege der Bild- und Tonübertragung nach § 128a ZPO durchgeführt werden können.[105] Die Vergabekammer darf außerdem unter der vereinfachten Voraussetzung, dass dies der Beschleunigung dient, nach Lage der Akten entscheiden.[106] Das Beschwerdegericht darf im Ausnahmefall ebenfalls nach Lage der Akten entscheiden, insbesondere, wenn dies der Beschleunigung dient und kein unmittelbarer Eindruck der Parteien oder direkter Austausch des tatsächlichen und rechtlichen Vortrags erforderlich ist.[107] Das Beschwerdegericht hat in der Sache stets selbst zu entscheiden und seine Beschwerdeentscheidung innerhalb von sechs Monaten ab Eingang der sofortigen Beschwerde zu treffen und zu begründen.[108]

Bei der Entscheidung nach § 168 Abs. 1 GWB, welche Maßnahmen geeignet sind, um eine Rechtsverletzung zu beseitigen und eine Schädigung der betroffenen Interessen zu verhindern, hat die Vergabekammer den Zweck nach § 1 BwBBG, die besonderen Verteidigungs- und Sicherheitsinteressen sowie die unmittelbare Stärkung der Einsatzfähigkeit der Bundeswehr zu berücksichtigen.[109] Im Rahmen weiterer Entscheidungen und Abwägungen der Nachprüfungsinstanzen, bspw. nach § 169 Abs. 2 Satz 1 GWB über die vorzeitige Gestattung des Zuschlags oder nach § 173 Abs. 2 Satz 1 GWB über die Verlängerung der aufschiebenden Wirkung, ist der Zweck des § 1 BwBBG ebenfalls zu berücksichtigen.[110] Die besonderen Verteidigungs- und Sicherheitsinteressen überwiegen dabei in der Regel, wenn der öffentliche Auftrag im unmittelbaren Zusammenhang mit der unmittelbaren Stärkung der Einsatzfähigkeit der Bundeswehr steht.[111]

B. Fazit

Auftraggeber werden bei Beschaffungen im Verteidigungs- und Sicherheitsbereich mit einem vielschichtigen und anspruchsvollen Rechtsrahmen konfrontiert. Bei näherer Betrachtung eröffnet dieser Rechtsrahmen dem Auftraggeber weitreichende Handlungsspielräume, um Beschaffungen im Verteidigungs- und Sicherheitsbereich zügig und bedarfsgerecht umzusetzen. Die derzeit geltenden vergaberechtlichen Bestimmungen im Verteidigungs- und Sicherheitsbereich stehen damit der Intention des Gesetzgebers, die Einsatzfähigkeit der Bundeswehr unverzüglich und schnellstmöglich zu stärken[112], nicht entgegen. Auftraggeber sind allerdings gut beraten, die einschlägigen rechtlichen Bestimmungen, die ihm diese weitreichenden Handlungsspielräume eröffnen, im Einzelfall sorgfältig zu prüfen und sämtliche Entscheidungen ausführlich und nachvollziehbar zu dokumentieren.

97 Amtliche Begründung der Bundesregierung zum Entwurf eines Gesetzes zur Beschleunigung von Beschaffungsmaßnahmen für die Bundeswehr (Bundeswehrbeschaffungsbeschleunigungsgesetz – BwBBG), BT-Drucks. 20/2353 v. 21.06.2022, S. 15.
98 § 3 Abs. 1 Satz 2, Abs. 3 Satz 2 BwBBG.
99 § 3 Abs. 4 Satz 1 BwBBG.
100 § 3 Abs. 4 Satz 2, Abs. 5 BwBBG.
101 § 4 Abs. 1 Satz 1 BwBBG.
102 § 7 Abs. 2 BwBBG.
103 § 7 Abs. 3 und 4 BwBBG.
104 §§ 4 Abs. 1 Satz 2, 7 Abs. 5 BwBBG.
105 §§ 5 Abs. 1 Satz 2, 6 Abs. 2 Satz 2 BwBBG.
106 § 5 Abs. 1 Satz 1 BwBBG.
107 § 6 Abs. 2 Satz 1 BwBBG.
108 § 6 Abs. 5 Satz 1 und 3 BwBBG.
109 § 5 Abs. 2 BwBBG.
110 §§ 5 Abs. 3 Satz 1 und Satz 3, 6 Abs. 1 Satz 1 und Abs. 3 Satz 1 BwBBG.
111 §§ 5 Abs. 3 Satz 2 und Satz 4, 6 Abs. 1 Satz 2 und Abs. 3 Satz 2 BwBBG.
112 Amtliche Begründung der Bundesregierung zum Entwurf eines Gesetzes zur Beschleunigung von Beschaffungsmaßnahmen für die Bundeswehr (Bundeswehrbeschaffungsbeschleunigungsgesetz – BwBBG), BT-Drucks. 20/2353 v. 21.06.2022, S. 10.

Schutz Kritischer Infrastrukturen im Vergaberecht

von Rechtsanwalt Johannes Baumann und Rechtsanwalt Julian Groenick, Düsseldorf*

A. Einleitung

Der Schutz Kritischer Infrastrukturen (KRITIS) ist essenziell, um zentrale gesellschaftliche Funktionen aufrechtzuerhalten. Die Bedeutung hat in den letzten Jahren zugenommen. Gerade die fortschreitende Digitalisierung, die damit einhergehende Gefahr von Cyberangriffen, das verstärkte Auftreten von Naturkatastrophen und geopolitische Konflikte stellen die öffentliche Hand vor große Herausforderungen. Angesichts zunehmender Bedrohungslagen ist der fortlaufende Schutz Kritischer Infrastrukturen unerlässlich. Das Vergaberecht übernimmt eine Schlüsselrolle bei der Beschaffung von Leistungen zur Sicherung

* Heuking Kühn Lüer Wojtek Partnerschaft mit beschränkter Berufshaftung von Rechtsanwälten und Steuerberatern.

und Aufrechterhaltung Kritischer Infrastrukturen. Dieser Beitrag stellt die gesetzlichen Grundlagen zum Schutz Kritischer Infrastrukturen im europäischen und nationalen Kontext sowie ausgewählte vergaberechtliche Schnittstellen dar und zeigt Regelungspflichten und -möglichkeiten auf, die im Rahmen von Vergabeverfahren zum Schutz Kritischer Infrastrukturen zur Verfügung stehen.

B. Rechtlicher Rahmen

I. Begriff „Kritische Infrastruktur"

Leistungsfähige Kritische Infrastrukturen bilden nach der nationalen Strategie zum Schutz Kritischer Infrastrukturen die Lebensadern moderner, leistungsfähiger Gesellschaften.[1] Danach handelt es sich um „Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden".[2] Die ständige Verfügbarkeit funktionierender Infrastrukturen wird in der Gesellschaft als selbstverständlich angesehen, ihr Ausfall kann hingegen in kürzester Zeit zu erheblichen Störungen des öffentlichen Lebens, zu wirtschaftlichen Schäden und Gefährdungen der öffentlichen Sicherheit führen. Nicht nur Terrorismus, Krieg und kriminelle Handlungen, sondern auch natürliche Ereignisse und menschliches und technisches Versagen können die Funktionsfähigkeit gefährden.[3] Die EU-Kommission zählt die Sicherheit Kritischer Infrastrukturen vor physischen und Cyberangriffen zu den größten Risiken für die wirtschaftliche Sicherheit Europas.[4]

Das Verständnis, was unter den Begriff Kritische Infrastrukturen fällt, variiert. Eine einfachgesetzliche Definition der Kritischen Infrastruktur enthält das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) und führt Sektoren der Kritischen Infrastruktur auf, unter anderem Energie, Telekommunikation, Transport und Ernährung.[5] Teilweise wird auch die Aufrechterhaltung des Staates und die Funktionsfähigkeit der Verwaltung unter den Begriff „Kritische Infrastruktur" gefasst, da auch ihr Ausfall die öffentliche Sicherheit gefährden kann.[6]

II. Rechtliche Grundlagen und aktuelle Entwicklungen

Bei akuten Bedrohungen für Kritische Infrastrukturen steht dem Staat zunächst das Gefahrenabwehrrecht zur Verfügung, um Schäden zu vermeiden. Das umfasst insbesondere die Befugnisse der Sicherheitsbehörden auf Bundes- und Landesebene, um präventiv auf Gefahren zu reagieren.

Neben dem Gefahrenabwehrrecht ist der Schutz Kritischer Infrastrukturen in einer Vielzahl von gesetzlichen Vorgaben außerhalb des Vergaberechts vorgesehen. Bisher zielen die Vorgaben außerhalb des Vergaberechts insbesondere auf den Schutz der IT-Sicherheit von Betreibern Kritischer Infrastrukturen ab. Zentral sieht das BSIG das Bundesamt für Sicherheit in der Informationstechnik (BSI) für den Schutz von Informationssicherheit vor.[7] Nach § 10 Abs. 1 BSIG legt das Bundesministerium des Innern, für Bau und Heimat (BMI) durch Rechtsverordnung[8] fest, welche Einrichtungen, Anlagen oder Teile im Einzelnen als Kritische Infrastrukturen gelten. Maßgeblich ist danach, ob sich der Ausfall auf die Versorgungssicherheit einer großen Zahl an Personen auswirkt, was in der Regel der Fall ist, wenn mind. 500.000 oder mehr Personen durch die jeweilige Infrastruktur versorgt werden.[9] Das BSI stellt zudem technische Richtlinien bereit, die den Stellen des Bundes bei Vergabeverfahren als Rahmen für die Entwicklung sachgerechter Anforderungen an Auftragnehmer und IT-Produkte dienen. Die Anforderungen sollen Auftraggebern im Vorfeld von Vergabeverfahren aufzeigen, wie sie Eignungs- und Leistungsanforderungen formulieren können, um ein hohes Sicherheitsniveau zu gewährleisten.[10]

Die europäische NIS2- Richtlinie[11] und die CER-Richtlinie[12] reformieren die bestehenden gesetzlichen Vorgaben zum Schutz Kritischer Infrastrukturen. Die NIS2-Richtlinie schafft einen einheitlichen europäischen Rechtsrahmen für Cybersicherheitsanforderungen Kritischer Infrastrukturen, um das Funktionieren des Binnenmarkts zu gewährleisten. Danach müssen die Mitgliedstaaten insbesondere nationale Cybersicherheitsstrategien verabschieden, zentrale Anlaufstellen benennen sowie Pflichten in Bezug auf das Cybersicherheitsrisikomanagement festlegen. Die neue CER-Richtlinie zielt darauf ab, die physische Resilienz kritischer Einrichtungen zu stärken, indem sie einheitliche Mindestverpflichtungen für kritische Einrichtungen sowie Aufsichtsmaßnahmen festlegt.

Beide Richtlinien wurden am 27.12.2022 im Amtsblatt der EU veröffentlicht mit einer Umsetzungspflicht bis Oktober 2024. In einigen Ländern, wie Belgien, Kroatien, Italien und Litauen, gelten bereits die neuen Anforderungen, in Deutschland hingegen noch nicht.[13] Die Umsetzung steht nun zumindest auf Bundesebene bevor, wobei mit einer Umsetzung nicht vor Herbst 2025 zu rechnen ist. Die NIS2-Richtlinie wird durch das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz[14] umgesetzt, das insbesondere das BSIG in wesentlichen Teilen neu fasst.[15] Das neue KRITIS-Dachgesetz[16] setzt die CER-Richtlinie um. Das Bundeskabinett hat beide Gesetze beschlossen. Sie befinden sich derzeit noch im parlamentarischen Abstimmungsprozess. Die neuen Vorgaben fokussieren sich auf die Begriffe „kritische Anlage" und „kritische Dienstleistungen". Eine kritische Anlage ist danach eine Anlage, die für die Erbringung einer kritischen Dienstleistung erforderlich ist. Eine kritische Dienstleistung ist eine solche, die zur Versorgung der Allgemeinheit in den Sektoren, deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen würde, erforderlich ist.[17]

III. Vergaberechtliche Bezüge

Der Schutz Kritischer Infrastrukturen weist in einigen Bereichen Bezüge zum Vergaberecht auf.

Während das BSIG die technischen und organisatorischen Anforderungen an den Schutz Kritischer Infrastrukturen festlegt, schafft das Vergaberecht den rechtlichen Rahmen für die Beschaffung der hierfür notwendigen Leistungen. Diese können eng mit der Funktionsfähigkeit oder dem Schutz Kritischer Infrastrukturen i.S.d. BSIG zusammenhängen und den Betrieb Kritischer Infrastrukturen selbst betreffen. Vergaberechtliche Bezüge bestehen jedoch auch darüber hinaus bei der Vergabe von Neben- und Hilfsleistungen, die erforderlich sind, um Kritische Infrastrukturen wiederherzustellen oder diesen dienen, aber nicht unmittelbar vom

1 Bundesministerium des Innern, Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie), Stand: 17.06.2009, S. 2.

2 Bundesministerium des Innern, Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie), Stand: 17.06.2009, S. 3.

3 Bundesministerium des Innern, Schutz Kritischer Infrastrukturen – Basisschutzkonzept, 2. Aufl. 2005, S. 10.

4 Europäische Kommission, Gemeinsame Mitteilung an das Europäische Parlament, den Europäischen Rat und den Rat über eine „Europäische Strategie für wirtschaftliche Sicherheit" v. 20.06.2023, JOIN(2023) 20 final.

5 § 2 Abs. 10 BSIG; zum Begriffsverständnis: Glade, in: Kipker/Reusch/Ritter, 1. Aufl. 2023, BSI-KritisV § 1 Rdnr. 1.

6 So bspw. das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Sektoren und Branchen KRITIS, https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/Sektoren-Branchen/sektoren-branchen_node.html, zuletzt abgerufen am: 13.01.2025; auch die NIS2-Richtlinie stuft die öffentliche Verwaltung als Sektor mit hoher Kritikalität ein, vgl. Anhang I Nr. 10 NIS-2-Richtlinie; ebenso die CER-Richtlinie und das KRITIS-Dachgesetz, hierzu Martini/Botta, LKV 2024, 293.

7 Das BSIG ist bereits im Jahr 1991 in Kraft getreten und trotz steigender Sicherheitsanforderungen bis zum Jahr 2009 nahezu unverändert geblieben, vgl. BT-Drucks. 16/11967, S. 10.

8 Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV).

9 Glade, in: Kipker/Reusch/Ritter, 1. Aufl. 2023, BSI-KritisV § 1 Rdnr. 54.

10 Entwurf und Begründung zum Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes, BT-Drucks. 16/11967, S. 16; Brandenburg, in: Kipker/Reusch/Ritter, 1. Aufl. 2023, BSIG § 8 Rdnr. 16 ff.

11 Richtlinie 2022/2555/EU des Europäischen Parlaments und des Rates v. 14.12.2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148, ABl. L 333 v. 27.12.2022.

12 Richtlinie 2022/2557/EU des Europäischen Parlaments und des Rates v. 14.12.2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates, ABl. L 333 v. 27.12.2022.

13 Europäische Kommission, Pressemitteilung v. 28.11.2024, https://germany.representation.ec.europa.eu/news/cybersicherheit-und-resilienz-kritischer-einrichtungen-vertragsverletzungsverfahren-gegen-2024-11-28_de, zuletzt abgerufen am: 13.01.2025.

14 Entwurf und Begründung zum Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung, BT-Drucks. 20/13184.

15 Entwurf und Begründung zum Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung, BT-Drucks. 20/13184, S. 10–71.

16 Entwurf und Begründung zum Gesetz zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen, BT-Drucks. 550/24; hierzu Kipker/Dittrich, MMR 2023, 481.

17 Entwurf und Begründung zum Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung, BT-Drucks. 20/13184, S. 16; Entwurf und Begründung zum Gesetz zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen, BT-Drucks. 550/24, S. 9 f.

engeren Begriff des BSIG und der konkretisierenden Verordnung erfasst sind. Dabei ermöglicht das Vergaberecht, Anforderungen in die Ausschreibungsbedingungen aufzunehmen, insbesondere in Form von Eignungs- und Ausführungsbedingungen, um sicherzustellen, dass Leistungen nur an geeignete Bieter vergeben werden und den gesetzlichen Vorgaben wie den Sicherheits- und Resilienzanforderungen des BSIG entsprechen.

1. Beseitigung von Schäden

Sind Kritische Infrastrukturen beschädigt oder drohen Beschädigungen, erlaubt das Vergaberecht schnelle Reaktionen. Ist die öffentliche Hand auf die Mitwirkung von Privaten angewiesen, um beschädigte Infrastrukturen wiederherzustellen oder unmittelbar drohende Schäden abzuwenden, ist in der Regel die Wahl des Verhandlungsverfahrens ohne Teilnahmewettbewerb zulässig, da es sich um äußerst dringliche, zwingende Gründe im Zusammenhang mit Ereignissen handelt, die nicht voraussehbar waren.[18] Das ist bspw. der Fall bei Leistungen zur Behebung von Sturm- und Brandschäden oder zur Bewältigung von Krisen.[19] Erforderlich ist eine drohende gravierende Beeinträchtigung für die Allgemeinheit und die staatliche Aufgabenerfüllung für den Fall, dass ein reguläres Vergabeverfahren durchgeführt würde.[20] Dabei dürfen dem öffentlichen Auftraggeber die die Notlage begründenden Umstände grundsätzlich nicht selbst zuzurechnen und für ihn nicht vorhersehbar sein.[21] Bei Aufgaben der Daseinsvorsorge, die auf Kritische Infrastrukturen angewiesen ist, gilt hingegen ein gelockerter Maßstab: Dringlichkeit kann hier auch dann vorliegen, wenn Auftraggeber die Dringlichkeit selbst zu verantworten haben. In solchen Fällen überwiegt die Aufrechterhaltung der Versorgung gegenüber der Frage nach der Vorhersehbarkeit oder Zurechenbarkeit der Ursache.[22] Auch bei Dringlichkeit ist jedoch immer noch so viel Wettbewerb wie möglich zu schaffen. So kann es zwar zulässig sein, auf eine europaweite Ausschreibung zu verzichten, aber dennoch erforderlich, mehrere Angebote einzuholen, soweit dies nach den Umständen des Einzelfalls zumutbar ist.[23] Der zügigen Beseitigung von Schäden jeglicher Art steht das Vergaberecht daher nicht entgegen.

Auch auf nationaler Ebene gelten bei gravierenden Schäden vergaberechtliche Erleichterungen, etwa durch temporäres Erhöhen von Schwellenwerten bei Direktvergaben, insbesondere zur Wiederherstellung von Infrastrukturen nach Naturkatastrophen wie Flutschäden.

2. Aufbau und Betrieb Kritischer Infrastrukturen

Der Aufbau und der Betrieb Kritischer Infrastrukturen erfordern nicht nur die Reaktion auf drohende oder bereits eingetretene Beeinträchtigungen der Funktionsfähigkeit, sondern auch ein kontinuierliches Weiterentwickeln, Warten und Schützen anhand aktueller Bedrohungsszenarien.

In erster Linie sind dabei die Betreiber von Kritischen Infrastrukturen verpflichtet, den Schutz Kritischer Infrastrukturen und deren Funktionsfähigkeit sicherzustellen und Vorkehrungen zur Störungsvermeidung zu treffen.[24] Sind die Betreiber von Kritischen Infrastrukturen selbst öffentliche Auftraggeber, sind sie verpflichtet, die steigenden gesetzlichen Anforderungen umzusetzen, insbesondere die eigene (IT-) Infrastruktur krisensicher zu gestalten und zudem einen angemessenen physischen Schutz ihrer Liegenschaften und kritischer Anlagen zu gewährleisten.[25] Nehmen Kommunen bspw. Aufgaben der öffentlichen Daseinsvorsorge wahr und betreiben etwa ein eigenes Krankenhaus oder sind Trinkwasserversorger und Abfallentsorger, können sie unter die KRITIS-Betreiber fallen.[26]

Insbesondere die zunehmende Bedrohungsintensität für die IT-Sicherheit von Kritischen Infrastrukturen stellt die öffentliche Hand vermehrt vor Herausforderungen und wirkt sich gerade im Hinblick auf Zertifizierungen und die Vertraulichkeit von Unterlagen auf Vergabeverfahren aus. Im Koalitionsvertrag setzte sich die gescheiterte Regierung daher noch zum Ziel, kritische Technologien und Infrastrukturen besser zu schützen sowie Standards und Beschaffung daran auszurichten, um in strategisch wichtigen Bereichen unabhängiger und weniger verwundbar zu sein.[27]

18 Vgl. § 14 Abs. 4 Nr. 3 VgV, § 3a Abs. 3 Nr. 4 EU VOB/A; § 13 Abs. 2 Nr. 4 SektVO.

19 Völlink, in: Ziekow/Völlink, 5. Aufl. 2024, VgV § 14 Rdnr. 62; Pünder, in: Pünder/Schellenberg, 3. Aufl. 2019, VgV § 14 Rdnr. 71.

20 BayObLG, Beschl. v. 20.01.2022 – Verg 7/21 m.w.N.

21 OLG Düsseldorf, Beschl. v. 15.02.2023 – VII-Verg 9/22.

22 OLG Frankfurt a.M., Beschl. v. 30.01.2014 – 11 Verg 15/13 m.w.N.

23 OLG Rostock, Beschl. v. 11.11.2021 – 17 Verg 4/21; OLG Karlsruhe, Beschl. v. 04.12.2020 – 15 Verg 8/20.

24 Entwurf und Begründung zum Gesetz zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen, BT-Drucks. 550/24, zu § 3, S. 33; s.a. § 8a BSIG zu Betreiberpflichten.

25 Entwurf und Begründung zum Gesetz zur Umsetzung der Richtlinie (EU)2022/2557 und zur Stärkung der Resilienz kritischer Anlagen, BT-Drucks. 550/24, § 13 Abs. 1 Nr. 2, S. 14.

26 Martini/Botta, LKV 2024, 293 (295).

C. Vergaberechtliche Vorgaben bei Beschaffungen im Zusammenhang mit Kritischer Infrastruktur

I. Anwendbares Vergaberecht und Ausnahmetatbestände

Das Vergaberecht sieht für bestimmte Aufträge im Zusammenhang mit Kritischen Infrastrukturen Ausnahmen von der Ausschreibungspflicht vor. Das betrifft insbesondere Aufträge im militärischen Bereich und zum Schutz wichtiger Sicherheitsinteressen sowie bestimmte Konzessionsvergaben. Eine einheitliche Begriffsverwendung, welche Leistungen der „Kritischen Infrastruktur" i.S.d. BSIG und der konkretisierenden Verordnung dienen, enthält das Vergaberecht nicht. Vielmehr ist im Einzelfall zu prüfen und festzustellen, ob eine Leistung den Betrieb Kritischer Infrastrukturen i.S.d. BSIG betrifft oder hierzu in einem sachlichen Zusammenhang steht.

Bei Betreibern Kritischer Infrastrukturen in den Bereichen Wasser, Elektrizität, Gas, Wärme und Verkehr handelt es sich häufig um Sektorenauftraggeber gem. § 100 Abs. 1 Gesetz gegen Wettbewerbsbeschränkungen (GWB), die entweder selbst originäre öffentliche Auftraggeber sind (Nr. 1), oder um natürliche oder private Personen, die über ein ausschließliches Recht verfügen (Nr. 2 Buchst. a)) oder ihre Tätigkeit unter dem beherrschenden Einfluss öffentlicher Auftraggeber ausüben (Nr. 2 Buchst. b)). Bei Auftragsvergaben zum Zwecke der Sektorentätigkeit unterliegen die Betreiber grundsätzlich gem. § 1 der Sektorenverordnung (SektVO). Aufträge von Sektorenauftraggebern, die nicht unmittelbar mit ihrer Sektorentätigkeit zusammenhängen, sind nach den allgemeinen vergaberechtlichen Vorgaben zu vergeben. Bei der Vergabe von Konzessionen, bspw. für den Betrieb von Infrastrukturen im Gas-, Strom-, oder Wasserbereich, findet hingegen – vorbehaltlich der Ausnahmen gem. § 149 GWB – die Konzessionsvergabeverordnung (KonzVgV) Anwendung.

Unter Anlegung eines weiten Begriffsverständnisses von „Kritischer Infrastruktur", das nicht auf die im BSIG genannten Bereiche beschränkt ist, bestehen vergaberechtliche Ausnahmetatbestände. So fällt zwar die militärische Infrastruktur nicht in den Anwendungsbereich des BSI,[28] ist jedoch unfraglich für die Sicherheit Kritischer Infrastrukturen notwendig. Im Fall von Militärausrüstungen und damit in Zusammenhang stehenden Leistungen ist bspw. gem. § 104 Abs. 1 GWB kein Vergabeverfahren erforderlich. Gleiches gilt für Aufträge, die im Rahmen eines Verschlusssachenauftrags vergeben werden. Auch Dienstleistungen im Bereich des Katastrophenschutzes, des Zivilschutzes oder der Gefahrenabwehr, die von gemeinnützigen Organisationen oder Vereinigungen erbracht werden, dürfen Auftraggeber gem. § 107 Abs. 1 Nr. 4 GWB ohne Vergabeverfahren vergeben. Im Hinblick auf den Schutz wesentlicher Sicherheitsinteressen der Bundesrepublik Deutschland ist § 107 Abs. 2 GWB relevant. Hierunter fallen insbesondere Aufträge und Konzessionen, bei denen im Rahmen von Vergabeverfahren Auskünfte erteilt würden, deren Preisgabe geeignet wäre, die nationale Sicherheit zu gefährden. In diesen Fällen kann Art. 346 Abs. 1 Buchst a) und b) AEUV einschlägig sein. Die Anforderungen des Art. 346 AEUV finden auch in § 117 GWB Berücksichtigung. Dieser stellt Aufträge, die wesentliche Sicherheitsinteressen betreffen, vergaberechtsfrei, ohne dass es sich um verteidigungs- oder sicherheitsspezifische Leistungen im engeren Sinne handelt.

Nach § 117 GWB unterfallen zudem bestimmte Aufträge, die Verteidigungs- oder Sicherheitsaspekte umfassen, ohne jedoch verteidigungs- oder sicherheitsspezifische Aufträge zu sein, nicht dem Vergaberecht. Das ist nach Nr. 1 der Vorschrift der Fall, soweit der Schutz wesentlicher Sicherheitsinteressen der Bundesrepublik Deutschland

27 Koalitionsvertrag 2021–2025 zwischen der Sozialdemokratischen Partei Deutschlands (SPD), Bündnis 90/Die Grünen und den Freien Demokraten (FDP), S. 105.

28 § 2 Abs. 10 BSIG.

nicht durch weniger einschneidende Maßnahmen gewährleistet werden kann, zum Beispiel durch Anforderungen, die auf den Schutz der Vertraulichkeit der Informationen abzielen, die der öffentliche Auftraggeber im Rahmen eines Vergabeverfahrens zur Verfügung stellt. Hierzu zählt bspw., schutzbedürftige leistungsspezifische Informationen nur den im Rahmen eines Teilnahmewettbewerbs ausgewählten qualifizierten und ggf. sicherheitsüberprüften Unternehmen zur Verfügung zu stellen.[29] Wird die Vergabe und die Ausführung eines Auftrags für geheim erklärt oder erfordert sie nach den Rechts- oder Verwaltungsvorschriften besondere Sicherheitsmaßnahmen, kommt eine Ausnahme vom Vergaberecht nach Nr. 3 der Vorschrift in Betracht. Vorrangig sind öffentliche Auftraggeber jedoch verpflichtet, weniger einschneidende Maßnahmen vorzuziehen, zum Beispiel durch Anforderungen zum Schutz der Vertraulichkeit von Informationen.

Darüber hinaus sieht das Vergaberecht Ausnahmen für den Betrieb öffentlicher Kommunikationsnetze und die Bereitstellung elektronischer Kommunikationsdienste vor. Diese Leistungen unterliegen gem. § 116 Abs. 2 GWB nicht dem Vergaberecht, wenn der Hauptzweck der Aufträge in der Bereitstellung bzw. dem Betrieb besteht und es sich um ein elektronisches Kommunikationsnetz handelt, das ganz oder überwiegend der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste dient.[30]

Die Ausnahme nach § 149 Nr. 9 GWB betrifft Konzessionen im Wassersektor. Dazu gehören die Bereitstellung, der Betrieb oder die Nutzung von Netzen zur Trinkwasserversorgung sowie damit verbundene Tätigkeiten wie die Abwasserbeseitigung oder Wasserbauprojekte. Der Wassersektor ist ein zentraler Bestandteil der Daseinsvorsorge und eine unverzichtbare Kritische Infrastruktur. Diese Ausnahme schafft Spielraum für eine etwas flexiblere Beschaffung außerhalb des Kartellvergaberechts.[31]

Greift im Einzelfall keine der genannten Ausnahmevorschriften ein, ist das Vergaberecht zu beachten. Überschreitet der geschätzte Auftragswert die Schwellenwerte für europaweite Ausschreibungen, richten sich die Vorgaben nach dem Kartellvergaberecht.

II. Anforderungen in Vergabeverfahren

Im Folgenden werden die Handlungsspielräume und Anforderungen in den verschiedenen Phasen eines typischen Vergabeverfahrens mit einem Fokus auf das Kartellvergaberecht dargestellt. Diese gelten nicht nur für Auftragsvergaben mit Bezug zu Kritischen Infrastrukturen i.S.d. BSIG, sondern sind auf eine Vielzahl sicherheitsrelevanter Vergabeverfahren übertragbar.[32]

1. Sicherstellung von IT-Schutz und Vertraulichkeit bei elektronischen Vergaben

Bei Vergabeverfahren in Zusammenhang mit Kritischen Infrastrukturen besteht oftmals ein Spannungsfeld zwischen der Pflicht, die Vergabeunterlagen umfassend frei zugänglich bereitzustellen und der Notwendigkeit, vertrauliche Informationen zu schützen.

Auf der ersten Stufe sind öffentliche Auftraggeber gefordert, zu entscheiden, welche Unterlagen und Informationen sie den Bewerbern bzw. Bietern zu welchem Zeitpunkt des Vergabeverfahrens zur Verfügung stellen müssen. Das Ziel der Informationssicherheit ist, dass nur diejenigen, die eine Information tatsächlich benötigen, Zugriff darauf erhalten sollen („Kenntnis nur, wenn nötig"). Dies kann allerdings im Konflikt zu den Vorgaben des Vergaberechts stehen. Die Vergabeunterlagen sind gem. § 41 Abs. 1 VgV grundsätzlich unentgeltlich, uneingeschränkt, vollständig und direkt online bereitzustellen. Allerdings bietet § 41 Abs. 3 VgV[33] dem Auftraggeber die Möglichkeit, in der Auftragsbekanntmachung oder in der Aufforderung zur Interessensbestätigung anzugeben, welche Maßnahmen zum Schutz der Vertraulichkeit von Informationen ergriffen werden und wie der Zugang zu den Vergabeunterlagen erfolgt.

29 Hölzl, in: Röwekamp/Kus/Portz/Prieß, 5. Aufl. 2020, GWB § 117 Rdnr. 15.

30 Antweiler, in: Ziekow/Völlink, 5. Aufl. 2024, GWB § 116 Rdnr. 29.

31 Dennoch folgt aus den primärrechtlichen Grundsätzen, dass solche Wasserkonzessionen in einem wettbewerblichen Verfahren zu vergeben sind, vgl. hierzu OLG Düsseldorf, Urt. v. 23.03.2018 – VI-2 U (Kart) 6/16 und Urt. v. 13.06.2018 – VI-2 U (Kart) 7/16.

32 Das Europäische Parlament „bedauert" in diesem Kontext in seiner Entschließung v. 17.01.2024 zu den sicherheits- und verteidigungspolitischen Auswirkungen des Einflusses Chinas auf die kritische Infrastruktur in der Europäischen Union (2023/2072(INI)), „das Fehlen einer angemessenen Überprüfung der Risiken einer Einmischung in die Vergabe öffentlicher Aufträge im Zusammenhang mit Sicherheitsausrüstung".

33 Vgl. auch § 41 Abs. 1 Satz 3 SektVO, § 8 Abs. 3 VOB/A VS.

Die Vorschrift legt weder fest, welche Schutzmaßnahmen der Auftraggeber wählen kann, noch wie ein alternativer Zugriff auf die Vergabeunterlagen zu gewähren ist. Ebenso wenig definiert die Vorschrift das erforderliche Maß an Vertraulichkeit, das bestehen muss, damit der Auftraggeber alternative Wege zu § 41 Abs. 1 VgV beschreiten darf. Dem Auftraggeber steht bei der Entscheidung, ob und welche Informationen als vertraulich anzusehen sind, ein Beurteilungsspielraum zu, der von den Nachprüfungsinstanzen nur eingeschränkt überprüfbar ist.[34] Dies dürfte insbesondere für sensible Informationen über Kritische Infrastrukturen oder Verfahren gelten, bspw. im IT-Bereich oder bei der Offenlegung von Einsatz-, Lage- oder Evakuierungsplänen.[35]

Daher kann der Auftraggeber die Überlassung von vertraulichen Vergabeunterlagen von der Sicherstellung der Geheimhaltung abhängig machen. Hierzu kann er die Abgabe einer entsprechenden Vertraulichkeits- bzw. Verschwiegenheitserklärung gem. § 5 Abs. 3 Satz 2 VgV in Betracht ziehen. Regelmäßig dürfte es im Verhandlungsverfahren mit Teilnahmewettbewerb sachgerecht sein, die Verschwiegenheitserklärung bereits im Rahmen des Teilnahmewettbewerbs zu fordern und die vertraulichen Informationen erst den ausgewählten Bietern im Rahmen der Angebotsphase zur Verfügung zu stellen. Denn erst nach Abschluss des Teilnahmewettbewerbs kann der öffentliche Auftragnehmer sicherstellen, dass der die Verschwiegenheitserklärung abgebende Bewerber vertrauenswürdig ist, da zu diesem Zeitpunkt zumindest bestätigt wurde, dass keine Ausschlussgründe gegen das Unternehmen vorliegen.[36]

In bestimmten Fällen darf der öffentliche Auftraggeber den Bewerbern bzw. Bietern den Zugang zu sicherheitsrelevanten Vergabeunterlagen erst nach Vorliegen weiterer Voraussetzungen gewähren. Dies ist insbesondere der Fall, wenn den Bewerbern bzw. Bietern im Rahmen des Vergabeverfahrens oder der Auftragsausführung der Zugang zu Verschlusssachen gewährt werden muss.

Im Geltungsbereich der VSVgV konkretisiert § 7 VSVgV[37] die Anforderungen des Sicherheitsüberprüfungsgesetzes (SÜG) und der darauf erlassenen Verwaltungsvorschriften.[38] Gem. § 7 Abs. 3 VSVgV müssen Auftraggeber bereits vor Gewährung des Zugangs zu Verschlusssachen des Geheimhaltungsgrades „VS-VERTRAULICH" oder höher von einem Bewerber, Bieter oder bereits in Aussicht genommenen Unterauftragnehmern einen Sicherheitsbescheid vom Bundesministerium für Wirtschaft und Energie oder von entsprechenden Landesbehörden sowie Verpflichtungserklärungen zum Verschlusssachenschutz verlangen. Muss einem Bewerber, Bieter oder bereits in Aussicht genommenen Unterauftragnehmer für den Teilnahmeantrag oder das Erstellen eines Angebots der Zugang zu Verschlusssachen des Geheimhaltungsgrades „VS-NUR FÜR DEN DIENSTGEBRAUCH" gewährt werden, verlangen Auftraggeber gem. § 7 Abs. 2 VSVgV bereits vor Gewährung dieses Zugangs die Verpflichtungserklärungen zum Verschlusssachenschutz.[39]

2. Eignung und Zertifizierung

Die Auswahl angemessener Eignungskriterien spielt bei der Konzeption und Durchführung von Vergabeverfahren im Zusammenhang mit Kritischen Infrastrukturen eine wesentliche Rolle, um Mindestanforderungen sicherzustellen und den Bewerber-/Bieterkreis anhand sachgerechter Kriterien einzuschränken.

a) Eigenerklärungen

Zum Nachweis der Eignung verlangt der öffentliche Auftraggeber gem. § 48 Abs. 2 Satz 1 VgV von den Bietern Eigenerklärungen. In Fällen, in denen eine Überprüfung der Eignung durch den Auftraggeber aus zeitlichen Gründen oder aufgrund fehlender Sachkunde faktisch nicht möglich ist, darf er auch Fremdbelege wie Zertifikate zum Nachweis der Eignung fordern.

34 Franzius, in: Pünder/Schellenberg, Vergaberecht, 3. Aufl. 2019, VgV § 41 Rdnr. 17.

35 Wichmann, in: Ziekow/Völlink, 5. Aufl. 2024, VgV § 41 Rdnr. 42; MünchKomm.-Schmidt, zum Wettbewerbsrecht, 4. Aufl. 2022, VgV § 41 Rdnr. 25.

36 Wichmann, in: Ziekow/Völlink, 5. Aufl. 2024, VgV § 41 Rdnr. 41.

37 Vgl. hierzu ausführlich Jäger, VergabeR, Sonderheft für Beschaffung in Verteidigung und Sicherheit, 2024, 644.

38 Allgemeine Verwaltungsvorschrift zum SÜG (SÜG-AVV) und Verschlusssachenanweisung (VSA).

39 Zur Rechtmäßigkeit der Aufhebung einer Sicherheitsermächtigung die den Zugang zu von einem Mitgliedstaat als Verschlusssachen eingestuften Informationen ermöglicht EuGH, 29.07.2024, C-185/23.

§ 48 Abs. 2 Satz 1 VgV legt fest, dass zur Nachweisführung der Eignung grundsätzlich die Vorlage einer Eigenerklärung akzeptiert wird. Die Verwendung des Wortes „grundsätzlich" verdeutlicht jedoch, dass im Einzelfall anstelle einer Eigenerklärung auch Fremdbelege zulässig sein können. Zudem nennt § 48 Abs. 1 VgV ausdrücklich Unterlagen in Form von Bescheinigungen und sonstigen Nachweisen, die zum Nachweis der Eignung gefordert werden dürfen.[40]

b) Zertifizierungen

Die Einhaltung von Normen der Qualitätssicherung ist für öffentliche Auftraggeber von zentraler Bedeutung, um die Qualität und Sicherheit der beauftragten Leistungen zu gewährleisten, insbesondere im Zusammenhang mit der Vergabe von Leistungen, die Kritische Infrastrukturen betreffen. Hierbei spielen Bescheinigungen über die Einhaltung von Qualitätssicherungsnormen, wie sie in den einschlägigen europäischen Normen festgelegt und von akkreditierten Stellen zertifiziert sind, eine entscheidende Rolle.[41]

Zunächst darf der öffentliche Auftraggeber – z.B. gem. § 49 VgV bzw. § 28 VSVgV – als Beleg für die Einhaltung von Normen der Qualitätssicherung Bescheinigungen über die vom Bewerber oder Bieter einzuhaltenden Normen der Qualitätssicherung von Qualitätssicherungssystemen verlangen. Hierzu gehören vor allem – aber nicht ausschließlich – die Qualitätsmanagementsysteme der Normenreihe DIN EN ISO 9000 und Zertifikate nach DIN EN ISO 27001.[42] Gleichwertige Bescheinigungen von akkreditierten Stellen aus anderen Staaten sind dabei anzuerkennen.

Im Bereich der IT-Sicherheit ist das BSI gem. § 9 Abs. 1 BSIG die nationale Zertifizierungsstelle der Bundesverwaltung.[43] Nach § 3 Abs. 3 BSIG kann das BSI Betreiber Kritischer Infrastrukturen auf deren Ersuchen bei der Sicherung ihrer Informationstechnik beraten und unterstützen oder auf qualifizierte Sicherheitsdienstleister verweisen. Nach Eigenangabe des BSI umfassen die von ihm angebotenen Leistungen die Zertifizierung von Produkten, die Zertifizierung von Managementsystemen und die Zertifizierung der Kompetenzfeststellung von Personen.[44]

Der gem. § 9 Abs. 5 BSIG für die Zertifizierung von IT-Sicherheitsdienstleistern geltende Abs. 4 sieht vor, dass das Zertifikat erteilt wird, wenn es den vom Bundesamt festgelegten Kriterien entspricht. Gem. § 18 Abs. 3 Nr. 4 BSIZertV enthält das Zertifikat des IT-Sicherheitsdienstleisters den technischen Geltungsbereich oder die technischen Geltungsbereiche der Zertifizierung unter Verweis auf die zugrunde gelegten Standardisierungsnormen.

Nach § 3 Abs. 1 Satz 2 Nr. 5 BSIG kommt dem BSI die Aufgabe zu, selbst Sicherheitszertifizierungen durchzuführen. Die Norm lässt offen, nach welchen Zertifizierungssystemen das BSI zertifiziert (z.B. Common Criteria). Es ist daher nicht auf selbst aufgestellte Zertifizierungssysteme beschränkt.[45]

c) Maßgeblicher Zeitpunkt der Eignungsnachweise/Zertifizierung

Im Rahmen von Ausschreibungsverfahren, insbesondere im Bereich der Kritischen Infrastruktur, besteht ein Spannungsfeld zwischen der Schaffung von Wettbewerb unter den Bietern und den hohen Sicherheitsanforderungen, die an Eignungsnachweise und Zertifikate gestellt werden. Einerseits ist das Ziel, den Wettbewerb zu fördern, um wirtschaftliche Angebote zu erhalten und Innovationen zu fördern. Andererseits müssen die Auftragnehmer strenge Sicherheitsanforderungen erfüllen, um die Zuverlässigkeit und Sicherheit der Kritischen Infrastruktur zu gewährleisten.

Für die Bewertung, ob ein Bieter die festgelegten Eignungsvoraussetzungen erfüllt, ist grundsätzlich der Zeitpunkt des Vertragsbeginns maßgeblich. Dies gilt, sofern der öffentliche Auftraggeber in der Bekanntmachung keinen anderen Zeitpunkt festgelegt hat. Eine Ausnahme besteht jedoch, wenn der Auftraggeber wirksam die Vorlage von Nachweisen für die Eignung bis zu einem bestimmten

40 VK Bund, Beschl. v. 28.05.2020 – VK 2-29/20.
41 VK Bund, Beschl. v. 19.07.2019 – VK 1-39/19.
42 BKartA, Beschl. v. 19.07.2019 – VK 1-39/19.
43 Zur Zulässigkeit der Zertifizierungen nach den IT-Sicherheitsstandards des BSI als Eignungsanforderung s.a.: Horn/Schuchert, MMR 2024, 926.
44 Bundesamt für Sicherheit in der Informationstechnik, Der Wert der Informationssicherheit: Zertifizierung und Anerkennung durch das BSI, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/zertifizierung-und-anerkennung_node.html, zuletzt abgerufen am: 13.01.2025.
45 Ritter, in: Kipker/Reusch/Ritter, 1. Aufl. 2023, BSIG § 3 Rdnr. 7.

Zeitpunkt gefordert und dies in der Vergabebekanntmachung entsprechend angegeben hat.[46]

Im Hinblick auf möglicherweise erforderliche Zertifizierungen müssen öffentliche Auftraggeber genau prüfen, zu welchem Zeitpunkt die Bieter diese nachweisen müssen. Insbesondere unter Berücksichtigung der Dauer eines Zertifizierungsprozesses kann es angemessen sein, dass die erforderliche Zertifizierung erst zum Zeitpunkt der Auftragsausführung vorliegen muss.

d) Auswirkungen auf Kritische Infrastruktur

Nach dem Vorstehenden ist es bei Ausschreibungen im Bereich Kritischer Infrastruktur daher besonders wichtig, die Eignungskriterien streng und frühzeitig zu prüfen. Die Zuverlässigkeit und Fachkunde sollten bereits bei Angebotsabgabe sichergestellt sein, um die Sicherheit und Kontinuität der Infrastruktur zu gewährleisten. Auch die „Leistungsfähigkeit" sollte bis zum Auftragsbeginn nachgewiesen werden, jedoch muss der Bieter vor Angebotsabgabe verbindlich erklären, dass ihm die notwendigen Mittel rechtzeitig zur Verfügung stehen. Dies stellt sicher, dass nur geeignete Unternehmen an der Ausführung beteiligt sind und die Kritische Infrastruktur geschützt bleibt.

3. Ausführungsbedingungen

Für den Schutz von Leistungen sind nach der Zuschlagserteilung und für die Dauer der Vertragsausführungen Ausführungsbedingungen gem. § 128 GWB relevant.

§ 128 Abs. 2 GWB erlaubt grundsätzlich, einzelfallbezogen Ausführungsbedingungen festzulegen, insbesondere zum „Schutz der Vertraulichkeit von Informationen". Relevant sind hierbei unter anderem sogenannte „No-Spy-Erklärungen", in denen die Bieter versichern müssen, dass sie nicht rechtlich zur Weitergabe von vertraulichen Daten an ausländische Geheimdienste und Sicherheitsbehörden – mit Ausnahme von Offenlegungspflichten gegenüber anderen ausländischen Stellen wie bspw. der Börsenaufsicht oder der Finanzverwaltung – verpflichtet sind.[47]

Der Regierungsentwurf zum Vergaberechtstransformationsgesetz sieht zudem vor, dass die besonderen Ausführungsbedingungen in § 128 Abs. 2 GWB um „Belange der Versorgungssicherheit" ergänzt werden, was die steigende Relevanz der Maßnahmen zum Schutz Kritischer Infrastruktur in Vergabeverfahren untermauert.[48]

D. Zusammenfassung und Ausblick

Der Schutz Kritischer Infrastrukturen erlangt zunehmend Bedeutung und wirkt sich auch auf Vergabeverfahren öffentlicher Auftraggeber aus. Das Vergaberecht schützt Kritische Infrastrukturen, indem es einige Leistungen in diesem Bereich vergaberechtsfrei stellt, enthält jedoch keine Sondervorgaben, die auf den Schutz Kritischer Infrastrukturen nach dem BSIG ausgerichtet sind. Ist das Vergaberecht bei Auftragsvergaben für Betrieb, Wartung oder sonstige Leistungen mit Bezug zu Kritischen Infrastrukturen anwendbar, müssen öffentliche Auftraggeber in jedem Einzelfall prüfen, welche Sicherheitsmaßnahmen zu ergreifen sind, um Kritische Infrastrukturen zu schützen und Informationssicherheit herzustellen. Die in Deutschland noch umzusetzenden NIS2 und CER-Richtlinien schaffen hierzu neue Vorgaben. Weitere Neuerungen mit vergaberechtlichen Bezügen schafft das von der EU geplante Binnenmarktnotfallinstrument.[49] Besonders hervorzuheben ist dabei die Möglichkeit der EU-Kommission, im Notfall im Namen der Mitgliedstaaten krisenrelevante Waren und Dienstleistungen zu beschaffen.[50]

46 OLG Düsseldorf, Beschl. v. 26.07.2018 – Verg 28/18; MünchKomm.-Hölzl, zum Wettbewerbsrecht, 4. Aufl. 2022, GWB § 122 Rdnr. 27.
47 Hierzu ausführlich: Gabriel/Bärenbrinker, VergabeR 2016, 166.
48 Gesetzentwurf der Bundesregierung zum Entwurf eines Gesetzes zur Transformation des Vergaberechts (Vergaberechtstransformationsgesetz – VergRTransfG) v. 20.12.2024; BT-Drucks. 20/14344, S. 70.
49 Europäische Kommission, Vorschlag für Verordnung des Europäischen Parlaments und des Rates zur Schaffung eines Notfallinstruments für den Binnenmarkt und zur Aufhebung der Verordnung (EG) Nr. 2679/98 des Rates, Art. 34 ff.
50 Ausführlich Conrad, in: Gabriel/Krohn/Neun, 4. Aufl. 2024, § 90 Rdnr. 5 ff.