75 Jahre Demokratie lebendig

Deutscher Bundestag
Wissenschaftliche Dienste

Sachstand

Auftragsvergaben im Cyberbereich mit Bezug zur inneren Sicherheit – Ausnahmetatbestände

Zur Rechtslage im Ausland

Auftragsvergaben im Cyberbereich mit Bezug zur inneren Sicherheit – Ausnahmetatbestände
Zur Rechtslage im Ausland

Aktenzeichen:	WD 7 - 3000 - 024/24
Abschluss der Arbeit:	13.06.2024
Fachbereich:	WD 7: Zivil-, Straf- und Verfahrensrecht, Medienrecht, Bau und Stadtentwicklung

Inhaltsverzeichnis

1. Einleitung und Rechtslage in Deutschland

Die EU-Richtlinie 2009/81/EG[1] verpflichtet staatliche Auftraggeber bei der Beschaffung bestimmter Leistungen im Verteidigungs- und Sicherheitsbereich zur Anwendung eines eigenständigen Vergaberechtsregimes. Auch bei Beschaffungsvorgängen, die sicherheitsspezifische Relevanz aufweisen, wie etwa der Beschaffung einer Virenschutzsoftware für Verwaltungen des Staates, findet mithin grundsätzlich das stark europarechtlich determinierte deutsche Vergaberecht Anwendung. Ziel des Vergaberechts ist die Schaffung einer transparenten Wettbewerbssituation.

Die Abgrenzung der unterschiedlichen vergaberechtlichen Anwendungsbereiche bei Beschaffungsvorgängen mit Bezug zur Cybersicherheit erfolgt im deutschen Recht im Einzelfall. Beschaffungsvorgänge im Bereich der inneren Sicherheit, die gemäß § 104 Absatz 3 des Gesetzes gegen Wettbewerbsbeschränkungen (GWB)[2] als Verschlusssachen (Einstufung nach § 4 des Gesetzes über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen (SÜG) in STRENG GEHEIM, GEHEIM, VS-VERTRAULICH, VS-NUR FÜR DEN DIENSTGEBRAUCH) qualifiziert werden, unterfallen dem Begriff der sicherheitsspezifischen öffentlichen Aufträge und werden in einem förmlichen Vergabeverfahren gemäß der §§ 104 und 144ff. GWB und nach den Vorschriften der Vergabeverordnung Verteidigung und Sicherheit (VSVgV)[3] vergeben. Im Rahmen dieses Vergabeverfahrens werden Maßnahmen und Instrumente genutzt, die insbesondere dem Vertraulichkeitsschutz innerhalb des Vergabeverfahrens dienen.

Für Sicherheitsvergaben, die nicht als Verschlusssachen eingestuft werden, gilt das reguläre Vergaberegime nach §§ 115 ff. GWB sowie die Vergabeverordnung (VgV)[4]. Die Durchführung eines förmlichen Vergabeverfahrens ist hier ebenfalls erforderlich. Bestimmte Aufträge im Sicherheitsbereich bleiben im deutschen Recht jedoch insgesamt vom Vergaberecht ausgenommen. Der Beschaffungsbedarf der öffentlichen Hand kann demnach in Einzelfällen derart sicherheitskritisch und -sensibel sein, dass ein förmliches Vergabeverfahren schlicht nicht durchgeführt werden kann.

---

1 EU-Richtlinie 2009/81/EG, abrufbar unter: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32009L0081 (Stand dieser und nachfolgender Internetquellen: 13.06.2024).

2 Gesetz gegen Wettbewerbsbeschränkungen in der Fassung der Bekanntmachung vom 26. Juni 2013 (BGBl. I S.1750, 3245), das zuletzt durch Artikel 2 des Gesetzes vom 22. Dezember 2023 (BGBl. 2023 I Nr. 405) geändert worden ist, abrufbar unter: https://www.gesetze-im-internet.de/gwb/GWB.pdf.

3 Vergabeverordnung Verteidigung und Sicherheit vom 12. Juli 2012 (BGBl. I S. 1509), die zuletzt durch Artikel 2 der Verordnung vom 7. Februar 2024 (BGBl. 2024 I Nr. 39) geändert worden ist, abrufbar unter https://www.gesetze-im-internet.de/vsvgv/.

4 Vergabeverordnung vom 12. April 2016 (BGBl. I S. 624), die zuletzt durch Artikel 1 der Verordnung vom 7. Februar 2024 (BGBl. 2024 I Nr. 39) geändert worden ist, abrufbar unter: https://www.gesetze-im-internet.de/vgv_2016/.

So enthält § 107 Absatz 2 GWB einen allgemeinen Ausnahmetatbestand für Vergaben, die Art. 346 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV)[5] unterfallen. § 145 GWB enthält weitere besondere Ausnahmetatbestände für Auftragsvergaben im Bereich der Sicherheit (u.a. für verteidigungs- oder sicherheitsspezifische Aufträge, die zum Zweck nachrichtendienstlicher Tätigkeiten oder an ausländische Regierungen vergeben werden). § 117 GWB enthält daneben weitere Ausnahmen für Aufträge, die nicht unter den Begriff des sicherheitsspezifischen Auftrags fallen, gleichwohl aber Sicherheitsaspekte aufweisen.

Aufgrund von sachlichen Überschneidungen der Ausnahmen kommt es teilweise zu Abgrenzungsschwierigkeiten. Im Ergebnis zielen alle gesetzlichen Ausnahmetatbestände jedoch darauf ab, den Schutz vertraulicher Daten vor Weitergabe und Offenlegung an unbefugte Dritte möglichst effektiv zu verhindern. Da der Verzicht auf ein Vergabeverfahren im wettbewerbsfokussierten Vergaberecht nur als ultima ratio in Betracht kommt, ist eine restriktive Auslegung aller Ausnahmen geboten.[6] Folglich bedarf es bei der Berufung auf Ausnahmetatbestände einer Abwägung im Einzelfall zwischen den öffentlichen Sicherheitsbelangen und den Interessen der Bieter unter Beachtung des Grundsatzes der Verhältnismäßigkeit.[7]

Vor diesem Hintergrund sind die Wissenschaftlichen Dienste des Deutschen Bundestages gebeten worden, die insoweit in anderen Ländern geltenden Regelungen bezüglich solcher Beschaffungsvorgänge darzustellen, die sicherheitsspezifische Relevanz aufweisen. Nachfolgend wird die Rechtslage ausgewählter Staaten daher summarisch wiedergegeben.[8]

2. Rechtslage im Ausland

2.1. Dänemark

Gemeinsam mit der dänischen Agentur für Digitalisierung veröffentlichte das dänische Zentrum für Cybersicherheit im Jahr 2022 den Leitfaden „Cybersicherheit in Lieferantenbeziehungen – Schützen Sie Ihr Unternehmen bei der Auslagerung des IT-Betriebs – von Anfang bis Ende“[9].

---

5 Konsolidierte Fassungen des Vertrags über die Europäische Union und des Vertrags über die Arbeitsweise der Europäischen Union (2016/C 202/01), abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:C:2016:202:FULL.

6 Ständige Rechtsprechung des EuGH; siehe aus jüngerer Zeit insbesondere EuGH Urteil vom 07.06.2012 – C–615/10, IBRRS 2012, 2179 Rn. 35; so auch Dreher, in: Immenga/Mestmäcker, Wettbewerbsrecht, 6. Auflage 2021, § 145 GWB Rn. 5.

7 Dreher, in: Immenga/Mestmäcker, Wettbewerbsrecht, 6. Auflage 2021, § 145 GWB Rn. 4.

8 Die Angaben zur Rechtslage im Ausland beruhen auf den Auskünften der jeweiligen Parlamentsverwaltung.

9 Leitfaden „Cybersicherheit in Lieferantenbeziehungen – Schützen Sie Ihr Unternehmen bei der Auslagerung des IT-Betriebs – von Anfang bis Ende“ in dänischer Sprache, abrufbar unter: https://www.cfcs.dk/globalassets/cfcs/dokumenter/vejledninger/Vejledning-cybersikkerhed-i-leverandorforhold_cfsc_digst-2022.pdf.

Darüber hinaus wurden verschiedene praktische Hilfsmittel für Behörden entwickelt, die die IT-Sicherheit bei öffentlichen IT-Beschaffungen und Ausschreibungen verbessern sollen.[10]

Betrifft die Ausschreibung kritische Infrastrukturen, können öffentliche Ausschreibungen in Dänemark der Genehmigungspflicht nach dem Investitionsschutzgesetz[11] unterliegen.

2.2. Frankreich

Für Aufträge im Verteidigungs- oder Sicherheitsbereich gelten besondere Vorschriften im französischen Gesetzbuch für das öffentliche Auftragswesen („code de la commande publique“)[12]. Dieser rechtliche Rahmen, der eine Ausnahme vom allgemeinen Recht darstellt, ist Gegenstand mehrerer Vorschriften, die von der französischen Nationalen Agentur für Cybersicherheit (ANSSI)[13] vorgelegt wurden.

Die ANSSI wurde im Juli 2009 gegründet und ist dem Generalsekretariat für nationale Verteidigung und Sicherheit (SGDSN) unterstellt. Die ANSSI unterstützt den Premierminister bei der Wahrnehmung seiner Aufgaben im Bereich der nationalen Verteidigung und Sicherheit und hat insbesondere folgende Dokumente vorgelegt:

– Die allgemeinen Sicherheitsrichtlinien („Référentiel général de sécurité – RGS“)[14]:

  Dieses Dokument enthält eine Reihe von Regeln für die Sicherheit von Informationssystemen, die für die Verwaltungsbehörden verbindlich sind. Diese Regeln betreffen vor allem die Produkte und Dienstleister, die von diesen Behörden zum Schutz ihrer Informationssysteme eingesetzt werden.

– Leitfaden für die Beschaffung RGS-qualifizierter Sicherheitsprodukte und Vertrauensdienste:

  Dieser Leitfaden wurde von der ANSSI in Absprache mit dem Staatlichen Beschaffungsamt (SAE) und der Direktion für Rechtsfragen (DAJ) des französischen Wirtschafts- und Finanzministeriums ausgearbeitet und erleichtert den Behörden die Einhaltung des allgemeinen

---

10 Leitfäden und Vorlagen etwa zum Lieferantenmanagement unter dem Abschnitt „Leverandørstyring“ in dänischer Sprache, abrufbar unter: https://www.sikkerdigital.dk/myndighed/vejledninger-og-skabeloner.

11 Investeringsscreeningsloven (Investitionsschutzgesetz), abrufbar in dänischer Sprache unter: https://www.retsinformation.dk/eli/lta/2023/1256; Erläuterungen zum Genehmigungsverfahren nach dem Investitionsschutzgesetz in dänischer Sprache unter: https://erhvervsstyrelsen.dk/ansoegning-om-tilladelse-i-forbindelse-med-en-offentlig-udbudsproces.

12 Code de la commande publique, abrufbar in französischer Sprache unter: https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000037701019/.

13 Website der Agence nationale de la sécurité des systèmes d'information (ANSSI), abrufbar in französischer Sprache unter: https://cyber.gouv.fr/.

14 Website der Agence nationale de la sécurité des systèmes d'information (ANSSI), „Achat de produits de sécurité et de services de confiance qualifiés dans le cadre du RGS“, abrufbar in französischer Sprache unter: https://cyber.gouv.fr/publications/achat-de-produits-de-securite-et-de-services-de-confiance-qualifies-dans-le-cadre-du.

Referenzrahmens für die Sicherheit: Es legt im Sinne des Kodex für das öffentliche Auftragswesen die Methodik für die Beschaffung von Sicherheitsprodukten (Verschlüsselungsgeräte, Smartcards, Firewalls, Schlüsselverwaltungsinfrastrukturen usw.) und Vertrauensdiensten (Anbieter von elektronischen Zertifizierungsdiensten, Audit-Anbieter usw.) fest, die selbst im Rahmen der RGS qualifiziert wurden.

Der Leitfaden zur Beschaffung von RGS-konformen Sicherheitsprodukten und Vertrauensdiensten richtet sich in erster Linie an alle Führungskräfte, die für die Beschaffung von Sicherheitsprodukten oder -diensten für Informationssysteme in Verwaltungen verantwortlich sind.

– Vertrauenswürdige Listen („listes de confiance“):

  Diese Listen sind wesentliche Elemente für die Schaffung von Vertrauen zwischen den Akteuren auf dem elektronischen Markt, da sie es den Nutzern ermöglichen, den qualifizierten Status und die Statushistorie von Vertrauensdiensteanbietern und ihren Diensten zu bestimmen.

  Die Vertrauenslisten der Mitgliedstaaten müssen mindestens die in den Artikeln 1 und 2 des Durchführungsbeschlusses (EU) 2015/1505 der Europäischen Kommission genannten Informationen enthalten. Die Mitgliedstaaten können in die vertrauenswürdigen Listen Informationen über nicht qualifizierte Vertrauensdiensteanbieter sowie Informationen über die von ihnen erbrachten nicht qualifizierten Vertrauensdienste aufnehmen. Es muss deutlich darauf hingewiesen werden, dass sie nicht gemäß der Verordnung (EU) Nr. 910/2014 qualifiziert sind.

Das französische Gesetzbuch für das öffentliche Auftragswesen („code de la commande publique“) sieht vor, dass für Verteidigungs- oder Sicherheitsaufträge bestimmte Verpflichtungen nicht gelten, wie beispielsweise die Bereitstellung technischer Unterlagen im Internet und die Verpflichtung, mehrere Unternehmen zum Wettbewerb aufzufordern. Um die Nichteinhaltung der Grundsätze des öffentlichen Auftragswesens (Transparenz der Informationen, Gleichheit der Bewerber) zu begrenzen, enthält Artikel L1113-1 des französischen Gesetzes über das öffentliche Auftragswesen[15] eine restriktive Definition dieser Aufträge:

„Ein Verteidigungs- oder Sicherheitsauftrag ist ein vom Staat oder einer seiner öffentlichen Einrichtungen geschlossener Vertrag, der Folgendes zum Gegenstand hat:

1. Lieferung von Ausrüstungsgegenständen, einschließlich Ersatzteilen, Bauteilen oder Unterbaugruppen, die zur Verwendung als Waffen, Munition oder Kriegsmaterial bestimmt sind, unabhängig davon, ob sie speziell für militärische Zwecke oder ursprünglich für zivile Zwecke konzipiert und anschließend für militärische Zwecke angepasst wurden;

15 Article L1113-1 du code de la commande publique, abrufbar in französischer Sprache unter: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000037703276.

2. Lieferung von Sicherheitsausrüstungen, einschließlich Ersatzteilen, Bauteilen oder Unterbaugruppen, die im Interesse der nationalen Sicherheit geschützte oder als geheim eingestufte Medien oder Informationen betreffen, erfordern oder enthalten;

3. Arbeiten, Lieferungen und Dienstleistungen, die unmittelbar mit den in den Ziffern 1 oder 2 genannten Ausrüstungen zusammenhängen, einschließlich der Lieferung von Werkzeugen, Prüfeinrichtungen oder spezifischer Unterstützung, und zwar während des gesamten oder eines Teils des Lebenszyklus der Ausrüstung. Als Lebenszyklus im Sinne dieses Absatzes gelten alle aufeinanderfolgenden Phasen, die die Ausrüstung durchlaufen kann, insbesondere Forschung und Entwicklung, industrielle Entwicklung, Produktion, Instandsetzung, Modernisierung, Umbau, Wartung, Logistik, Ausbildung, Erprobung, Rückzug, Demontage und Entsorgung;

4. Bau- und Dienstleistungen mit spezifisch militärischer Zweckbestimmung oder Bau- und Dienstleistungen für Sicherheitszwecke, die im Interesse der nationalen Sicherheit geschützte oder als Verschlusssache eingestufte Medien oder Informationen betreffen, erfordern oder enthalten.

Die in Artikel L. 3 dargelegten Grundsätze sollen bei der Anwendung auf Verteidigungs- oder Sicherheitsaufträge auch die Stärkung der europäischen verteidigungstechnologischen und -industriellen Basis gewährleisten.“

Im Bereich von Verteidigungs- oder Sicherheitsaufträgen ist in Artikel R.2322-5 des französischen Gesetzbuchs für das öffentliche Auftragswesen[16] festgelegt:

„Der Auftraggeber kann einen Auftrag ohne vorherige Bekanntmachung oder Ausschreibung vergeben, wenn der Auftrag nur an einen bestimmten Wirtschaftsteilnehmer vergeben werden kann, und zwar aus Gründen des Schutzes von Ausschließlichkeitsrechten oder aus technischen Gründen, wie z. B. besondere Interoperabilitäts- oder Sicherheitsanforderungen, die erfüllt werden müssen, um das Funktionieren der Streitkräfte oder der Sicherheitskräfte zu gewährleisten, oder wenn es für einen anderen Bewerber als den erfolgreichen Wirtschaftsteilnehmer technisch absolut unmöglich ist, die geforderten Ziele zu erreichen, oder wenn auf spezielles Know-how, spezielle Werkzeuge oder Ressourcen zurückgegriffen werden muss, die nur einem einzigen Wirtschaftsteilnehmer zur Verfügung stehen, insbesondere bei der nachträglichen Änderung oder Anpassung besonders komplexer Ausrüstungen.“

Aufträge im Bereich Verteidigung und Sicherheit werden auf der Website des französischen Wirtschaftsministeriums veröffentlicht.[17]

16 Article R2322-5 du code de la commande publique, abrufbar in französischer Sprache unter https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000037729135.

17 Ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique, Les marchés de défense ou de sécurité, abrufar in französischer Sprache unter: https://www.economie.gouv.fr/daj/marches-defense-securite-2020.

2.3. Niederlande

In der niederländischen „Arbeitsagenda wertorientierte Digitalisierung“[18] ist u. a. als Ziel festgeschrieben, dass Behörden und Regierungsstellen ausschließlich sichere Informations- und Kommunikationstechnik (IKT) -Produkte und -Dienstleistungen vom Markt nutzen und erwerben sollen (Agenda Titel 2.5 „Verbesserung der Cybersicherheit“).

Die niederländische Regierung nutzt außerdem ein Online-Instrument „Anforderungen an die öffentliche Beschaffung von Cybersicherheit“ („Inkoopeisen Cybersecurity Overheid“ (ICO)[19]), mit dem eine Reihe von spezifischer Informationssicherheitsanforderungen für Beschaffungen und Verträge mit IKT-Lieferanten zusammengestellt werden können, die erfüllt werden müssen. Auf diese Weise versucht die Regierung die Nachfrage nach digital sicheren IKT-Produkten und -Dienstleistungen anzuregen und ihre eigene Sicherheit zu erhöhen.[20]

Zurzeit wird zudem untersucht, ob die der ICO zugrunde liegenden Normen in der Gesetzgebung verankert werden können. Daneben wird eine Aufnahme dieser Normen in eine überarbeitete Version der Baseline Information Security Government („Baseline Informatiebeveiliging Overheid“ (BIO)[21]) diskutiert.[22]

Im Hinblick auf das Ziel der Beschaffung von digital sicheren IKT-Produkten und -Dienstleistungen, wurde ein Beschaffungsinstrument, der ICO-Wizard[23], entwickelt. Dieser bietet Unterstützung bei der Auswahl der richtigen Informationssicherheitsanforderungen und ermöglicht die Auswahl von Anforderungspaketen, die zu verschiedenen Arten von Produkten und/oder Dienstleistungen passen, die ausgeschrieben oder beschafft werden sollen. Ergänzt wird der Assistent durch „Privacy-by-Design-Anforderungen“, Anforderungen aus dem Polizeidatengesetz (Wet Politie Gegevens (WPO)[24], welches die Verarbeitung von polizeilichen Daten, die in einer Datei enthalten sind oder enthalten sein sollen durch die zuständige Behörde regelt), durch verpflichtende

---

18 Updated Values-Driven Digitalisation Work Agenda, abrufbar in englischer Sprache unter: https://www.digitaleoverheid.nl/wp-content/uploads/sites/8/2023/01/26234-Values-Driven-Digitalisation-Work-Agenda_English-TG.pdf.

19 Website Digitale Overheid, „Inkoopeisen Cybersecurity Overheid“, abrufbar in niederländischer Sprache unter: https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cybersecurity/inkoopeisen-cybersecurity-overheid/.

20 Website Baseline Informatiebeveiliging Overheid, „Veilig aanbesteden en inkopen: ICO-producten“, abrufbar in niederländischer Sprache unter: https://bio-overheid.nl/category/producten?product=ICOproducten.

21 Website Baseline Informatiebeveiliging Overheid, „Implementatie van de BIO“, abrufbar in niederländischer Sprache unter: https://www.bio-overheid.nl/.

22 Brief an die Abgeordnetenkammer: Integraler Überblick Digitalisierung 2023 - Verzamelbrief Digitalisering december 2023), S. 15, abrufbar in niederländischer Sprache unter: https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2023D51510&did=2023D51510.

23 Website Baseline Informatiebeveiliging Overheid, „ICO-Wizard“, abrufbar unter: https://bio-overheid.nl/ico-wizard/.

24 Wet Politie Gegevens (WPO), abrufbar in niederländischer Sprache unter: https://wetten.overheid.nl/BWBR0022463/2023-11-01.

staatliche Maßnahmen aus der Baseline Information Security Government (BIO) und durch Cybersecurity-Anforderungen aus den Allgemeinen Sicherheitsanforderungen („Algemene Beveiligingseisen Defensie Opdrachten“, ABDO).

Weiterführende Informationen sind in der niederländischen Cybersicherheitsstrategie 2024 – 2028[25] sowie auf der Internetseite von PIANOo[26] (Kompetenzzentrum für Beschaffung des Ministeriums für Wirtschaft und Klimapolitik) enthalten.

Gesetzliche Grundlagen zur Beschaffung durch die niederländische Regierung befinden sich im Gesetz über das öffentliche Beschaffungswesen 2012 (Aanbestedingswet 2012)[27], welches etwa die Beschaffung von Produkten, Dienstleistungen und Konzessionen durch den Staat, eine Provinz (regionale Behörde), eine lokale Behörde oder einen Wasserverband regelt sowie im Gesetz über das öffentliche Beschaffungswesen im Bereich Verteidigung und Sicherheit (Aanbestedingswet op defensie- en veiligheidsgebied)[28]. Letzteres Gesetz regelt die Koordinierung und die Verfahren für die Vergabe von Aufträgen für Bauleistungen, Lieferungen und Dienstleistungen im Bereich Verteidigung und Sicherheit.

Abschnitt 6a.8, Absatz 6 des Gesetzes über das öffentliche Beschaffungswesen 2012 (Aanbestedingswet 2012) legt fest:

> „Im Falle eines Auftrags, der sich auf eine Tätigkeit bezieht, auf die Teil 2a Anwendung findet, und auf eine andere Tätigkeit, auf die § 346 des Vertrags über die Arbeitsweise der Europäischen Union Anwendung findet, oder auf die das Vergaberecht im Bereich Verteidigung und Sicherheit Anwendung findet, kann die Fachgesellschaft:
>
> a. einen Auftrag ohne Anwendung von Teil 2a dieses Gesetzes vergeben, wenn diese Tätigkeit unter § 346 des Vertrags über die Arbeitsweise der Europäischen Union fällt, oder
>
> b. einen Auftrag entweder nach Teil 2a dieses Gesetzes oder nach dem Beschaffungsgesetz für den Bereich Verteidigung und Sicherheit vergeben, wenn diese Tätigkeit unter dieses Gesetz fällt.“

Abschnitt 2.16 des Gesetzes über das öffentliche Beschaffungswesen im Bereich Verteidigung und Sicherheit (Aanbestedingswet op defensie- en veiligheidsgebied) regelt:

> „Abweichend von den Abschnitten 2.1 bis 2.3 gelten die Bestimmungen dieses Gesetzes oder aufgrund dieses Gesetzes nicht für Aufträge,

---

25 Ministry of Justice and Security, National Coordinator for Counterterrorism and Security, Netherlands Cybersecurity Strategy 2022-2028, abrufbar in englischer Sprache unter: https://english.nctv.nl/topics/netherlands-cybersecurity-strategy-2022-2028.

26 Website von PIANOo, „Beschaffungsanforderungen für Informationssicherheit“, abrufbar in niederländischer Sprache unter: https://www.pianoo.nl/nl/sectoren/ict/inkopen-van-ict/inkoopeisen-voor-informatiebeveiliging.

27 Aanbestedingswet 2012, abrufbar in niederländischer Sprache unter: https://wetten.overheid.nl/BWBR0032203/2022-03-02/0.

28 Aanbestedingswet op defensie- en veiligheidsgebied, abrufbar in niederländischer Sprache unter: https://wetten.overheid.nl/BWBR0032898/2019-04-18/0.

a. deren Ausführung dazu führt, dass die beschaffende staatliche Stelle oder das beschaffende Unternehmen Informationen zur Verfügung stellen muss, deren Offenlegung dem wesentlichen Sicherheitsinteresse zuwiderläuft;

b. im Zusammenhang mit der Tätigkeit von Nachrichtendiensten;

c. die in den Rahmen eines Kooperationsprogramms zwischen dem Königreich der Niederlande und einem oder mehreren anderen Mitgliedstaaten fallen, das auf Forschung und Entwicklung im Hinblick auf die Entwicklung eines neuen Produkts abzielt, gegebenenfalls einschließlich der späteren Phasen eines vollständigen Lebenszyklus dieses Produkts oder eines Teils davon;

[…]

h. die von einer niederländischen staatlichen Stelle an eine staatliche Stelle eines anderen Staates vergeben werden und die unter Abschnitt 2.1 Buchstaben a, b oder c fallen, sofern sich diese Aufträge auf Bau- oder Dienstleistungen beziehen, oder d.“

2.4. Österreich

Die Rechtslage in Österreich entspricht im Wesentlichen der in Deutschland.

Im Bundesvergabegesetz (BVergG)[29] bestimmt § 9 BVergG, für welche Vergabeverfahren dieses Gesetz nicht gilt. Im konkreten Zusammenhang sind insbesondere § 9 Absatz 1 Ziffer 1, 4 und 7 BVergG beachtlich:

„(1) Dieses Bundesgesetz gilt nicht für

1. Aufträge im Verteidigungs- und Sicherheitsbereich, die dem BVergGVS 2012 unterliegen, sowie für Aufträge, die gemäß § 9 BVergGVS 2012 vom Geltungsbereich des BVergGVS 2012 ausgenommen sind,

[…]

4. Vergabeverfahren, sofern ein öffentlicher Auftraggeber aufgrund der Anwendung der Bestimmungen dieses Bundesgesetzes verpflichtet würde, Informationen zu übermitteln, deren Offenlegung nach Auffassung der Republik Österreich ihren wesentlichen Sicherheitsinteressen zuwiderlaufen würde (Art. 346 Abs. 1 lit. a AEUV),

5. Vergabeverfahren, deren Durchführung und Ausführung aufgrund von bundes- oder landesgesetzlichen Bestimmungen für geheim erklärt werden oder deren Durchführung und Ausführung aufgrund bundes- oder landesgesetzlicher Bestimmungen besondere Sicherheitsmaßnahmen erfordert und die dafür zuständige Behörde festgestellt hat, dass der Schutz der betreffenden wesentlichen Interessen nicht durch weniger einschneidende Maßnahmen gewährleistet werden kann,

---

29 Österreichisches Bundesgesetz über die Vergabe von Aufträgen (Bundesvergabegesetz 2018 – BVergG 2018), abrufbar unter: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010295.

[…]

7. Vergabeverfahren mit Verteidigungs- oder Sicherheitsaspekten, deren Durchführung anderen verpflichtenden Verfahrensregeln unterliegen und die festgelegt wurden

a) durch eine im Einklang mit dem AEUV geschlossene internationale Übereinkunft oder Vereinbarung zwischen der Republik Österreich und einem oder mehreren Drittstaaten über Leistungen für ein von den Vertragsparteien gemeinsam zu verwirklichendes oder zu nutzendes Projekt, oder

b) durch eine internationale, einen bestimmten Unternehmer betreffende Übereinkunft oder Vereinbarung im Zusammenhang mit dem Aufenthalt von Truppen, oder

c) durch eine internationale Organisation,

[…].“

Für Verfahren zur Beschaffung von Leistungen im Verteidigungs- und Sicherheitsbereich wurde das Bundesgesetz über die Vergabe von Aufträgen im Verteidigungs- und Sicherheitsbereich (Bundesvergabegesetz Verteidigung und Sicherheit 2012 – BVergGVS 2012)[30] erlassen.

2.5. Schweden

In Schweden gibt es keine ausdrücklichen Rechtsvorschriften für die Vergabe öffentlicher Aufträge im Zusammenhang mit der internen Cybersicherheit.

Das schwedische Gesetz über das öffentliche Auftragswesen (SFS 2016:1145)[31] regelt das öffentliche Beschaffungswesen. Es ist jedoch nicht anwendbar, wenn das Gesetz über das Beschaffungswesen im Bereich Verteidigung und Sicherheit (SFS 2011:1029)[32] gilt (vgl. Kapitel 3, Abschnitt 3 Ziffer 1 des schwedischen Gesetzes über das öffentliche Auftragswesen).

Gemäß Kapitel 3, Abschnitt 3, Punkt 2 des schwedischen Gesetzes über das öffentliche Beschaffungswesen wird eine Beschaffung, die ausdrücklich vom Anwendungsbereich des Gesetzes über das Beschaffungswesen im Bereich Verteidigung und Sicherheit ausgenommen ist, auch nicht durch das schwedische Gesetz über das öffentliche Beschaffungswesen geregelt. Dies bedeutet,

---

30 Österreichisches Bundesgesetz über die Vergabe von Aufträgen im Verteidigungs- und Sicherheitsbereich (Bundesvergabegesetz Verteidigung und Sicherheit 2012 – BVergGVS 2012), abrufbar unter: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20007693.

31 The Swedish Public Procurement Act (SFS 2016:1145) in schwedischer Sprache, abrufbar unter: https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/lag-20161145-om-offentlig-upphandling_sfs-2016-1145/; in englischer Sprache, abrufbar unter: https://www.konkurrensverket.se/globalassets/dokument/informationsmaterial/rapporter-och-broschyrer/informationsmaterial/swedish-public-procurement-act.pdf [Die Übersetzung enthält möglicherweise nicht alle aktuellen Änderungen der Rechtsvorschriften.].

32 The Swedish Act on Procurement in the area of defence and security (2011:1029) in schwedischer Sprache, abrufbar unter: https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/lag-20111029-om-upphandling-pa-forsvars-och_sfs-2011-1029/#K1.

dass es möglich ist, bestimmte Aufträge von den Beschaffungsanforderungen ganz auszuschließen. Jedoch gibt es keine spezifischen Bestimmungen, die Aufträge im Zusammenhang mit interner Cybersicherheit ausdrücklich von den Beschaffungsanforderungen ausschließen. Abhängig von der Art des jeweiligen Vertrags im Zusammenhang mit interner Cybersicherheit könnten sie jedoch unter die Ausnahmen für Beschaffungsanforderungen fallen, die in Kapitel 1 Abschnitt 7 bis 10 des Gesetzes über das Beschaffungswesen im Bereich Verteidigung und Sicherheit aufgeführt sind:

> „Abschnitt 7: Dieser Rechtsakt findet keine Anwendung, wenn die Artikel 36, 51, 52 oder 62 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) zur Anwendung kommen.
>
> Abschnitt 8: Dieses Gesetz gilt nicht für Beschaffungen, die besonderen Verfahrensregeln unterliegen
>
> 1. aufgrund eines völkerrechtlichen Vertrages oder Abkommens zwischen einem oder mehreren Staaten des Europäischen Wirtschaftsraums (EWR) und einem oder mehreren anderen Staaten
>
> 2. aufgrund eines internationalen Vertrags oder einer internationalen Übereinkunft über die Stationierung von Militärpersonal und über die Verpflichtungen eines Staates; oder
>
> 3. von einer internationalen Organisation angewandt werden, die Käufe für den Eigenbedarf tätigt, oder von einem EWR-Staat nach solchen besonderen Verfahrensregeln vergeben werden.
>
> Abschnitt 9: Bei Beschaffungen im Zusammenhang mit der Herstellung von oder dem Handel mit Waffen, Munition und Kriegsmaterial, die unter Artikel 346 Absatz 1 Buchstabe b AEUV fallen und auf die Abschnitt 7 oder 8 oder Abschnitt 10 Absatz 1 Nummern 2 bis 4 oder 10 keine Anwendung finden, kann die Regierung im Einzelfall Ausnahmen von den Bestimmungen dieses Gesetzes beschließen, die im Hinblick auf die wesentlichen Sicherheitsinteressen Schwedens erforderlich sind.
>
> Die schwedischen Streitkräfte und die schwedische Verwaltung für Verteidigungsmaterial können über die in Absatz 1 genannten Ausnahmen entscheiden, wenn die Beschaffung
>
> 1. sich auf eine Ergänzung einer Beschaffung bezieht, für die die Regierung zuvor eine Ausnahme gemäß Absatz 1 beschlossen hat,
>
> 2. Waren, Dienstleistungen oder Bauleistungen im Rahmen eines von Schweden abgeschlossenen internationalen Abkommens über die zwischenstaatliche Zusammenarbeit bei der Lieferung von Waren, Dienstleistungen oder Bauleistungen betrifft oder
>
> 3. einen Wert von nicht mehr als 200 000 000 SEK hat.
>
> Das schwedische Amt für Verteidigungsfunk kann über die im ersten Absatz genannten Ausnahmen entscheiden, wenn der Wert der Beschaffung 5.000.000 SEK nicht übersteigt. Gesetz (2023:253).
>
> Abschnitt 10: Dieses Gesetz ist nicht anwendbar auf Verträge

1. bei denen die Anwendung dieses Gesetzes einen öffentlichen Auftraggeber oder eine Einrichtung zur Erteilung von Auskünften verpflichten würde, deren Offenlegung den wesentlichen Sicherheitsinteressen Schwedens zuwiderlaufen würde,

2. die sich auf nachrichtendienstliche Tätigkeiten beziehen

[…]

6. die von einer anderen Regierung an eine Regierung vergeben werden und sich beziehen auf

(a) die Lieferung von militärischer Ausrüstung oder sensibler Ausrüstung

(b) Bau- und Dienstleistungen, die unmittelbar mit der unter Buchstabe a) genannten Ausrüstung zusammenhängen, oder

(c) Bau- und Dienstleistungen, die speziell für militärische Zwecke bestimmt oder von sensibler Beschaffenheit sind

[…].“

3. Fazit

Wie die vorhergehende Länderübersicht zeigt, bestehen in den meisten der dargestellten Länder Regelungen zur Beschaffung von Leistungen im Cyberbereich mit Bezug zur inneren Sicherheit, die der deutschen Rechtslage – aufgrund des europarechtlich determinierten Vergaberechts – in vielen Teilen ähneln. Die Ausgestaltung im Einzelfall – insbesondere im Hinblick auf konkrete Beschaffungsvorgänge, die sicherheitsspezifische Relevanz aufweisen – unterscheidet sich in der Reichweite jedoch im Detail. So haben etwa die Niederlande ein Online-Beschaffungsinstrument zur Unterstützung öffentlicher Auftraggeber bei der Beschaffung von Cybersicherheit entwickelt, wohingegen etwa Dänemark und Frankreich überwiegend Leitfäden und Richtlinien als Hilfestellung erstellt haben.

***