EIN STAATSGRUNDNETZ 2.0 – WETTBEWERBS- UND VERGABERECHTLICHE UMSETZUNG

Ralf Blaha / Jonas Pfister / Jakob Zanol

Ralf Blaha, Rechtsanwalt, Wissenschaftlicher Projektmitarbeiter, Universität Wien, Arbeitsgruppe Rechtsinformatik
Olsastraße 17, 9360 Friesach, AT
Blaha@digitalanwalt.at

Jonas Pfister, Wissenschaftlicher Projektmitarbeiter, Universität Wien, Arbeitsgruppe Rechtsinformatik
Schottenbastei 10-16/2/5, 1010 Wien, AT
Jonas.Pfister@univie.ac.at

Jakob Zanol, Wissenschaftlicher Projektmitarbeiter/Managing Scientist, Universität Wien, Arbeitsgruppe Rechtsinformatik
Schottenbastei 10-16/2/5, 1010 Wien, AT
Jakob.Zanol@univie.ac.at

Schlagworte: ***Staatsgrundnetz, Public-Private-Partnership (PPP), Wettbewerbsrecht, Vergaberecht, Kritische Infrastruktur, Resilienz, Netzausfall, KIRAS***

Abstract: *Ein Staatsgrundnetzes (SGN 2.0) soll gemäß seiner Konzeption i.S. eines Overlay-Netzes Schutz vor Netzausfällen bieten und die Erfüllung staatlicher Aufgaben ermöglichen. Ein resilientes SGN 2.0 hat aber keinesfalls bloß eine staatsrechtliche Dimension, sondern erfordert auch die Einbeziehung privatrechtlich organisierter Akteure (etwa im Rahmen einer Public-Private-Partnership). Hierzu ergeben sich jedoch wettbewerbs- und vergaberechtliche Fragen, die über die Konzeption eines SGN hinausgehen und allgemein den Schutz kritischer Infrastruktur durch kooperative Maßnahmen betreffen.*

1. Ein SGN 2.0 als "Public-Private-Partnership" (PPP)

Beim im Rahmen des KIRAS Forschungsprojekts Hammondorgel[1] konzipierten Staatsgrundnetz 2.0 (kurz: SGN 2.0) geht es im Wesentlichen um die Frage, wie man auf der Grundlage bereits vorhandener Netzwerkinfrastruktur zusätzliche Resilienz und Robustheit schafft.[2] Dies ist vor dem Hintergrund zu sehen, dass mit zunehmender Digitalisierung Informations- und Kommunikationstechnologien (IKT) eine wesentliche Grundlage – wenn nicht gar Grundvoraussetzung – für das Funktionieren staatlicher Aufgaben darstellt. Daher muss die zunehmende Abhängigkeit von IKT für die Bewältigung dieser Aufgaben adressiert werden. Das Ziel des SGN 2.0 Konzeptes ist es daher, die IKT auch bei einem Netzausfall aufrecht zu erhalten.

Es ist davon auszugehen, dass ein neues Staatsgrundnetz unter den aktuellen Rahmenbedingungen ein „*präventives kollaboratives und integriertes Zusammenarbeiten der wichtigsten Betreiber von Kommunikationsinfrastruktur in Österreich über Organisationsgrenzen hinweg, teilweise unter gemeinsamer Nutzung individuell bereitgestellter Netzwerkinfrastruktur und unter der Annahme unterschiedlicher Kernaufgaben und assoziierter Netzwerkqualitätsvorstellungen*" erfordert.[3] Ein solches präventives, kollaboratives und integriertes Zusammenarbeiten erfolgt im SGN 2.0 durch die sogenannte „Vermaschung" bereits bestehender Netzwerkstrukturen. Über ein eigenes „Overlay-Netz" ist es möglich, dass Organisation 1 selbst bei einem Netzausfall über das „Gastgebernetz" der Organisation 2 ihre interne Kommunikation leitet und daher diese im Krisenfall in der (robust gemachten) Arbeitsumgebung weiterführen kann (also ohne Wechsel zu einer

[1] Siehe https://www.kiras.at/gefoerderte-projekte/detail/hammondorgel (aufgerufen am 30.11.2021).

[2] Dieser Beitrag ist als komplementärer Beitrag zu Bühler, H./Latzenhofer, M./Poindl, P./Zanol, J., Ein Staatsgrundnetz 2.0 – Resilienz durch „Amtshilfe"?, in diesem Tagungsband, Weblaw, Bern 2022, S. 109 zu verstehen.

[3] Ebd.

dezidierten Notfallumgebung). In anderen Worten „borgt" sich Organisation 1 bei einem Netzausfall das Netz der Organisation 2.

Der Ausfall eines Netzes und damit der IKT ist ein nicht unerhebliches Schadensrisiko und hat selbstverständlich auch unabhängig davon, ob dieser staatliche oder private Akteure betrifft, disruptives Potential. Ist kritische Infrastruktur[4] von einem Netzausfall betroffen, so kann dies erhebliche gesamtgesellschaftliche Folgen nach sich ziehen.

Zum Schutz kritischer Infrastruktur wird in Österreich vielfach auf das Public-Private-Partnership-Konzept gesetzt. Dabei geht es um einen dauerhafte funktionierende Zusammenarbeit zwischen Staat, Wirtschaft und auch Wissenschaft[5], insbesondere aber zwischen Staat und „strategischen Unternehmen"[6] (kritischer Infrastruktur). Dahinter steckt die Überlegung, dass ein bereits bestehender Austausch, gemeinsam absolvierte Übungen und gemeinsame Schutzstandards erlauben, im Krisenfall direkt an dieser Kooperation anknüpfen zu können und damit Probleme kooperativ schnell und effizient zu lösen.

Auch das SGN 2.0 hat Ähnlichkeiten mit einer PPP. Es geht beim SGN 2.0 um eine Vermaschung wesentlicher Netzinfrastrukturen zum Vorteil aller beteiligter Partner (deren Netze dadurch wesentlich robuster werden). Soll das SGN 2.0 jedoch über den staatlichen Bereich hinausgehen und sollen private Akteure in das SGN 2.0 eingebunden werden, ergeben sich aber auch wesentlich komplexere und zum Teil noch ungelöste Rechtsfragen. Sind sowohl private als auch staatliche Akteure kooperative Partner in einem SGN 2.0, so geht es einerseits um die Frage, ob Unternehmen hier in einer marktbeeinflussenden Weise durch den Staat gefördert werden, andererseits um die Frage, unter welchen Voraussetzungen Leistungen von Unternehmen durch den Staat in Anspruch genommen werden können.

2. Wettbewerbsrechtliche Aspekte

Wenn private mit staatlichen Akteuren kooperieren, besteht stets das Risiko eines – wenn auch unwillentlichen oder unwissentlichen – Eingriffes in den freien Wettbewerb. Der freie Markt ist jedoch Schutzsubjekt des Wettbewerbsrechts.[7] Staatliche Eingriffe in ebendiesen gilt es zunächst zu vermeiden. Erfolgen sie dennoch, sind sie aber jedenfalls rechtfertigungsbedürftig.[8] Partizipieren private Partner an einer Version des Staatsgrundnetzes 2.0, führt dies zu einer gesteigerten Resilienz ihrer Netze. Basiert die Teilnahme auf einem freiwilligen System, in dem Anreize für eine Partizipation geschaffen werden, so könnte auch darin ein Vorteil für Partner gesehen werden. Eine Ex-Ante Beurteilung zum Vorhandensein bzw. zum Ausmaß eines tatsächlichen Vorteils und damit einer Wettbewerbsverzerrung ist diffizil. Dies ist dem Umstand geschuldet, dass der Vorteil keiner am Markt vorhandenen Leistung entsprechen würde.

Schutz vor Wettbewerbsverzerrungen bieten sowohl das materielle Unionsrecht, das nationale allgemeine Wettbewerbsrecht, als auch das sektorspezifische Recht im Telekommunikationsbereich. In Bezug auf das europäische Wettbewerbsrecht stellt sich zunächst grundlegend die Frage, ob der Sachverhalt überhaupt unter dem Gesichtspunkt des Wettbewerbsrechts zu betrachten ist. Da das SGN 2.0 prioritär die Wahrnehmung staatlicher Aufgaben im Krisenfall ermöglichen soll, könnte der Sachverhalt auch unter dem Aspekt des Katastrophenschutzes, der Aufrechterhaltung der inneren Ordnung oder der nationalen Sicherheit subsumiert werden. Nach Ansicht der Europäischen Kommission, finden die Binnenmarktvorschriften und Wettbewerbsregeln keine Anwendung auf wesentliche Staatsaufgaben.[9, 10] Dies gilt unter der Bedingung, dass die Tätig-

4 Auf den Begriff der kritischen Infrastruktur, wird unten in Abschnitt 4 noch eingegangen.
5 Siehe Bundeskanzleramt/Bundesministerium für Inneres, Österreichisches Programm zum Schutz kritischer Infrastrukturen, 2015, S. 14.
6 Ebd., S. 10, 14.
7 Wiebe (Hrsg.) Wettbewerbs- und Immaterialgüterrecht[3], Facultas, Wien 2016, S. 285.
8 Müller/Raschauer (Hrsg), Europäisches Wirtschaftslenkungs- und Regulierungsrecht, Verlag Österreich, Wien 2015, S. 1.
9 Europäische Kommission, Mitteilung „Leistungen der Daseinsvorsorge in Europa", Abl. C 2001/17, S. 9.
10 Kling, Staatliches Handeln, Daseinsvorsorge und Kartellrecht, FIW 2014/248, S. 19.

keiten keinen „wirtschaftlichen Charakter“ aufweisen. Keinen wirtschaftlichen Charakter weist jedenfalls eine lediglich nachfragende Tätigkeit auf, wenn Zieltätigkeit eine Kernaufgabe des Staates betrifft.[11] Bei einer dauerhaften Kooperation ist die Lage jedoch nicht derart eindeutig.

In einer solchen könnte abhängig von der Ausgestaltung aufgrund des weiten Wortlauts eine Absprache i.S.d. Art. 101 AEUV gesehen werden. Da das Wettbewerbsrecht unter anderem auch zum Ziel hat, Manipulation und Verfälschung des freien Marktes durch staatliche Maßnahmen zu unterbinden,[12] kann es ebenso auf öffentliche juristische Personen angewandt werden. Anders betrachtet könnte die Kooperation allerdings auch als staatliche Beihilfe i.S.d. Art. 107 AEUV klassifiziert werden. Dies kann jedenfalls nur dann vorliegen, wenn die ausgetauschten Leistungen keine Äquivalente darstellen.[13] Darüber hinaus hat der EuGH klargestellt, dass im Bereich staatlicher Infrastrukturmaßnahmen das Vorliegen einer Begünstigung davon abhängt, ob eine bestimmte Infrastrukturanlage wirtschaftlich nutzbar ist.[14]

Kommt man zum Schluss, dass die Voraussetzungen für einen der Tatbestände erfüllt sind, so besteht immer noch die Möglichkeit, dass eine Ausnahme zur Anwendung kommt. Eine solche kann in Art. 106 AEUV gesehen werden. Nach selbiger können Unternehmen mit Dienstleistungen von allgemeinem wirtschaftlichen Interesse (Daseinsvorsorge) betraut werden. Diesfalls wären die Unternehmen von den europäischen Wettbewerbsbestimmungen ausgenommen. Die Betrauung kann nicht nur durch Gesetz, sondern auch durch Vertrag erfolgen, sofern die vergaberechtlichen Bestimmungen eingehalten werden.[15]

3. Vergaberechtliche Aspekte

Vergaberechtliche Fragen stellen sich dann, wenn es im Rahmen des SGN 2.0 zur Beschaffung von Leistungen durch öffentliche Auftraggeber im Wege entgeltlicher Verträge kommt. Das ist z.B. dann der Fall, wenn ein Telekommunikationsunternehmen damit beauftragt wird, gegen Entgelt das eigene Netzwerk so anzupassen und zu konfigurieren, dass es mit anderen teilnehmenden Organisationen zusammengeschaltet werden kann. Erfolgt hingegen ein Beschaffungsvorgang im Rahmen des SGN 2.0 auf Basis eines Gesetzes, einer Verordnung oder einem individuellen Hoheitsakt wie z.B. einem Bescheid, kommt das Vergaberecht nicht zur Anwendung.[16]

Beim SGN 2.0 kommt sowohl die Anwendung des Bundesvergabegesetzes[17] (in der Folge „BVergG“) als auch die Anwendung des Bundesvergabegesetzes Verteidigung und Sicherheit[18] (in der Folge „BVergG-VS“) in Frage. Soweit Aufträge über „sensible Dienstleistungen“ vergeben werden – das sind Dienstleistungen, die einen Sicherheitszweck erfüllen oder Verschlusssachen verwenden, erfordern oder beinhalten[19] – so fallen diese Beschaffungen in den Anwendungsbereich des BVergGVS. Dies ist z.B. der Fall, wenn konzeptive oder architekturelle Merkmale des SGN 2.0, die bei der Einrichtung oder dem Betrieb der Staatsgrundnetzfunktionalität im Netzwerk eines Telekommunikationsunternehmen umzusetzen sind, aus Gründen der nationalen Sicherheit vor Offenlegung zu schützen sind. Ansonsten fallen die Aufträge in den Anwendungsbereich des BVergG.

---

11 Lewisch, In: Mayer/Stöger (Hrsg.), EUV/AEUV Art. 106 AEUV Rz. 16 (Stand 1.8.2013, rdb.at).

12 Rüffler/Steinwender, In: Holoubek/Potacs (Hrsg.), Öffentliches Wirtschaftsrecht[3],Verlag Österreich, Wien 2013, S. 565; vgl. hiezu im nationalen Recht auch die Pflicht zur Objektivität und Neutralität des Staates: Wiebe (Hrsg.), Wettbewerbs- und Immaterialgüterrecht[3], Facultas, Wien 2016, S. 307.

13 Sutter, In: Mayer/Stöger (Hrsg.), EUV/AEUV Art. 107 AEUV Rz. 35 (Stand 1.1.2014, rdb.at).

14 Bartosch, EU-Beihilfenrecht[2], Verlag C. H. Beck, München 2016, § 107 Abs. 1 AEUV Rz. 54 unter Verweis auf EuGH 26. September 2013, C-518/13, *London Taxi*, Rz. 50.

15 Lewisch, In: Mayer/Stöger (Hrsg.), EUV/AEUV Art. 106 AEUV Rz. 87 (Stand 1.8.2013, rdb.at).

16 Heid/Ring, In: Heid, S,/Reisner, H./Deutschmann D./Hofbauer B., Bundesvergabegesetz 2018, Verlag Österreich, Wien 2019 § 1 Rz 5 m.w.N.

17 BGBl. I Nr. 65/2018 i.d.F. BGBl. I Nr. 100/2018.

18 BGBl. I Nr. 10/2012 i.d.F. BGBl. I Nr. 100/2018.

19 § 3 Z. 30 BVergGVS.

Für die Umsetzung der Beschaffungsvorgänge im Rahmen des SGN 2.0 bietet sich das Open House-Modell an. Dieses ist mangels gesetzlicher Einschränkung sowohl im Anwendungsbereich des BVergG-VS als auch im Anwendungsbereich des BVergG zulässig. Dieses geht auf eine Entscheidung des EuGH zurück, in der jener ein Vertragsmodell geprüft hat, welches vorsah, dass alle die Zulassungskriterien erfüllenden interessierten Unternehmen zugelassen und mit jedem von ihnen übereinstimmende Vereinbarungen zu im Voraus festgelegten und nicht verhandelbaren Vertragsbedingungen abgeschlossen werden. Dieses Modell sah weiters vor, dass Verträge mit allen interessierten Unternehmen geschlossen werden können, ohne eine Auswahl zu treffen, und dass jedes andere Unternehmen, das diese Kriterien erfüllt, dem System während dessen Laufzeit zu denselben Bedingungen beitreten kann. Nach dem EuGH stellt ein solches Vertragssystem keinen öffentlichen Auftrag im Sinne der Vergaberichtlinie[20] für öffentliche Auftraggeber dar, sofern es im Einklang mit den Grundregeln des AEU-Vertrags, insbesondere der Nichtdiskriminierung, ausgestaltet und durchgeführt wird.[21]

Das Open House-Modell sieht keine Auswahl der besten Bieter, sondern die Einbeziehung aller Unternehmer vor, welche die vorab definierten Bedingungen erfüllen. Dieses Modell erscheint daher für das SGN 2.0, bei dem ein wesentlichsten Ziel die Mitarbeit möglichst vieler Telekommunikationsunternehmen ist, besonders geeignet.

Es gibt eine Reihe weiterer Verfahrensarten, die für die Beschaffung von Leistungen im Rahmen des SGN 2.0 in Frage kommen würden, wie dynamische Beschaffungssysteme[22], Innovationspartnerschaften[23] und Verhandlungsverfahren zum Abschluss von Rahmenvereinbarungen[24]. Dynamisches Beschaffungssystem und Innovationspartnerschaft haben jedoch den Nachteil, dass sie nur im BVergG, nicht aber im BVergG-VS vorgesehen sind; Innovationspartnerschaft und Verhandlungsverfahren haben den Nachteil, dass sie nicht auf Dauer ausgelegt sind, sondern eine Teilnahme nur innerhalb einer definierten Frist möglich ist. Alle diese Verfahrensarten verbindet schließlich der Nachteil, dass sie auf die Auswahl eines Bestbieters bzw. einer begrenzten Anzahl an Vertragspartnern ausgerichtet sind. Sie alle weisen daher im Hinblick auf die Zielsetzung des SGN 2.0 gegenüber dem Open House-Modell wesentliche Nachteile auf.

Die optimale Vertragsart, mittels der das SGN 2.0 umgesetzt wird, hängt in erster Linie von Art und Umfang des Leistungsaustausches sowie der Enge der Zusammenarbeit ab. Wenn auch PPPs regelmäßig in Form gemeinsamer Gesellschaften der öffentlichen und privaten Akteure umgesetzt werden, dürften im Falle des SGN 2.0 weniger weitgehende Dauerschuldverhältnisse wie Kooperationsvereinbarungen ausreichen.

4. Sonderfall „Kritische Infrastruktur“?

Da es sich bei jenen potenziellen Partnern eines SGN 2.0 mit einer relevanten eigenen Netzwerkinfrastruktur primär um kritische Infrastruktur handelt, stellt sich nach den vorherigen Ausführungen (insbesondere zum Wettbewerbsrecht) die Frage, ob eine Kooperation mit staatlichen Akteuren nicht ohnehin durch den jeweiligen Mitgliedstaat uneingeschränkt geregelt werden kann.

Die Frage, wieweit die Kompetenz der Mitgliedstaaten im Bereich der kritischen Infrastruktur geht, wird rechtsgebieteübergreifend diskutiert. Beispielsweise ermächtigt Art. 23 Datenschutz-Grundverordnung (DSGVO[25]) Mitgliedstaaten durch Rechtsvorschriften Beschränkungen für gewisse Pflichten und Rechte der

[20] Nunmehr 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 2014/94, S. 65.

[21] EuGH 2. Juni 2016, C-410/14, Falk; Öhler, M./Malin, D., EuGH: „Open House“-Modell zulässig – kein öffentlicher Auftrag, Recht der Wirtschaft 2016, S. 684.

[22] § 31 Abs 8 BVergG.

[23] § 31 Abs 10 BVergG.

[24] § 31 Abs 7 BVergG.

[25] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR, Abl. L 2016/119, S. 1.

Verordnung vorzusehen, wenn dies etwa zur Sicherstellung der „öffentlichen Sicherheit" erfolgt. Teilweise wird dazu vertreten, dass eine entsprechende Bestimmung in der DSGVO nicht erforderlich gewesen wäre, würden doch Angelegenheiten der „öffentlichen Sicherheit" ohnehin in die ausschließliche Regelungskompetenz der Mitgliedstaaten fallen.[26] Aufgrund des Grundsatzes der begrenzten Einzelermächtigung (Art. 5 EUV) wäre eine solche Regelung demnach sogar unzulässig. Es stellt sich die Frage, ob der Umstand, dass diese Bestimmung dennoch erlassen wurde, ein Umdenken dieser klaren Trennung von Kompetenzen bedingt, wurde die DSGVO doch von der großen Mehrzahl der Mitgliedstaaten angenommen. Dem ließe sich entgegenhalten, dass eine Überschreitung der Kompetenzen nicht zu einer Anpassung führen kann (i.S.d. Grundsatzes „*ex iniuria ius non oritur*"). Dieser Frage ungeachtet, muss anerkannt werden, dass der Katastrophenschutz und generell staatliche Aktivitäten zur Wahrung der öffentlichen Sicherheit in der Regel rechtliche „Querschnittsmaterien" betreffen, was notwendigerweise zu Abgrenzungsfragen zwischen nationalen und unionalen Kompetenzen führt. Dies gilt umgekehrt auch für das soeben aufgeworfene Rechtsgebiet des Datenschutzrechts, welches Anknüpfungspunkte zu allen übrigen Rechtsgebieten[27] hat. Daher erscheint eine Regelung wie jene des Art. 23 DSGVO für eine verhältnismäßige Konsolidierung sinnvoll.[28]

Die Frage nach der Einordnung der Kooperation zwischen staatlichen und privaten Akteuren bleibt im geltenden Recht unbeantwortet. Zwar finden sich in verschiedenen Rechtsgebieten „Freiräume" für Mitgliedstaaten – so auch im Wettbewerbsrecht – für entsprechende Maßnahmen, allerdings sind diese sehr eng gefasst[29] und die Anwendbarkeit auf das SGN 2.0 nicht hinreichend klar.[30]

Mitunter ist diese unklare Zuordnung auch der Grund, warum sich auf europäischer Ebene zu „kritischer Infrastruktur" derzeit (noch) kein umfassendes Regelungsregime findet. Dem erfolgreichen Vorstoß im Bereich der Sicherheit von Netz- und Informationssystemen (NIS-RL[31]) scheint jedoch nun auch eine umfassende Regelung zur Erhöhung der Resilienz kritischer Infrastruktur[32] zu folgen. Die derzeit in Geltung stehend EKI-Richtlinie regelt primär die Ermittlung von „Europäischen Kritischen Infrastrukturen" und enthält keine darüberhinausgehenden Regelungen für eine Zusammenarbeit von mitgliedstaatlichen Behörden und kritischer Infrastruktur.[33]

Im Ergebnis lässt sich wohl festhalten, dass die Zusammenarbeit zwischen staatlichen Behörden und privaten Akteuren (ob im Rahmen einer PPP oder auch ganz generell) nicht bereits deswegen pauschal dem Anwendungsbereich europäischer Vorgaben entzogen ist, weil es sich bei den privaten Akteuren um „kritische Infrastruktur" handelt. Die europäischen Regelungsvorstöße werden schließlich auch durch die Mitgliedstaaten mitgetragen, welche zunehmend eine einheitliche Vorgehensweise und europäische Kooperation begrüßen. Zusätzlich soll an dieser Stelle jedoch auch hervorgehoben werden, dass eine ausdrückliche Regelung auf

---

26 So etwa Peuker, In: Sydow, Europäische Datenschutzgrundverordnung: Handkommentar[2], Nomos, Baden-Baden 2018, Art. 23 Rz. 22; aA etwa Bäcker, In: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG: Kommentar[2], C.H. Beck, München 2018, Art. 23 Rz. 20.

27 Beachte jedoch die materiellen Abgrenzungen in Art 2 DSGVO zu anderen Rechtsakten.

28 So wohl auch Kieck/Pohl, Zum Anwendungsbereich des europäischen Datenschutzrechts, DuD 2017, S. 567.

29 Siehe oben Abschnitt 2.

30 Die Europäische Kommission führte aus, dass „nichtwirtschaftliche Tätigkeiten", die per se dem Staat vorbehalten sind (einschließlich der Wahrung der inneren und äußeren Sicherheit) von Binnenmarktvorschriften und Wettbewerbsregeln ausgenommen sind; vgl. Europäische Kommission, Mitteilung „Leistungen der Daseinsvorsorge in Europa", Abl C 2001/17, S. 9; da im Rahmen des SGN 2.0 jedoch durchaus eine geldwerte Leistung erfolgt (Stärkung der Resilienz des Netzes) ist die Übertragbarkeit auf das SGN 2.0 fraglich.

31 Siehe Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, Abl. L 2016/194, S. 1; siehe auch den Vorschlag zur Überarbeitung dieser Richtlinie: Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, ABl. L 2016/194, S. 1.

32 Siehe Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Resilienz kritischer Einrichtungen, COM(2020) 829 final.

33 Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern, ABl. L 2008/345, S. 75.

europäischer Ebene, welche die Zusammenarbeit von staatlichen Akteuren und kritischer Infrastruktur direkt adressiert, auch für die Mitgliedstaaten zusätzliche Rechtssicherheit verspricht. In diesem Sinne ist Art. 9 des Vorschlags für eine Richtlinie über die Resilienz kritischer Einrichtungen[34] zu begrüßen, der eine Kooperation zwischen kritischen Einrichtungen und staatlichen Akteuren ausdrücklich vorsieht.[35]

5. Fazit

Ein Staatsgrundnetz 2.0, das nicht nur staatliche Akteure untereinander verbinden, sondern auch strategische Unternehmen oder kritische Infrastruktur einbeziehen soll, wirft durchaus komplexe Rechtsfragen auf. Die hier thematisierten Fragestellungen sind jedoch stellvertretend für jede PPP mit dem Ziel kritische Infrastruktur zu schützen.

Zunächst zeigt sich, dass die gegenseitige Zurverfügungstellung von Netzkapazität (beschränkt für den jeweiligen Netzausfall) allen Partnern des SGN 2.0 einen Vorteil bringt, da diese von einer resilienteren bzw. robusteren Netzinfrastruktur profitieren. Hier stellt sich sowohl die Frage der Zulässigkeit des „*Gebens*“ an private Unternehmen, und zwar die Zurverfügungstellung von Netzkapazität, als auch die Frage der Zulässigkeit des „*Nehmens*“ von privaten Unternehmen, und zwar die Inanspruchnahme fremder Netzkapazität, durch staatliche Akteure.

Die Anwendbarkeit des Wettbewerbsrechts kann nicht bereits deshalb ausgeschlossen werden, weil sich eine Maßnahme auf kritische Infrastruktur bezieht. Die im europäischen Wettbewerbsrecht bereits vorgesehenen Ausnahmen[36] sind allerdings im Fall des SGN 2.0 nicht eindeutig anwendbar, sodass hier eine gewisse Rechtsunsicherheit besteht. Die Notwendigkeit, auch bei der Unterstützung kritischer Infrastruktur die wettbewerbsrechtlichen Bestimmungen zu berücksichtigen wird auch im neuen Richtlinien-Entwurf zur Erhöhung der Resilienz kritischer Einrichtungen festgehalten.[37]

Darüber hinaus können staatliche Akteure auch nicht ohne weiteres Leistungen privater Unternehmen in Anspruch nehmen. Sofern diese Inanspruchnahme nicht auf Gesetzen, Verordnungen oder individuellen Hoheitsakten beruht, sondern entgeltliche Verträge geschlossen werden, unterliegt sie dem Vergaberecht. Bei sensiblen Dienstleistungen sind die Vorgaben des Bundesvergabegesetzes Verteidigung und Sicherheit einzuhalten, bei sonstigen Leistungen die Vorgaben des Bundesvergabegesetzes. Sollte das Vergaberecht einschlägig werden, erscheint den Autoren die Umsetzung im Wege eines Open House-Modells am zielführendsten; dieses ermöglicht den Vertragsabschluss mit allen Unternehmen, welche vorab festgelegte Bedingungen zur Teilnahme am SGN 2.0 erfüllen.

Die Autoren kommen somit zum Schluss, dass die Umsetzung des SGN 2.0 unter Einbeziehung privater Unternehmen (PPP) auf Basis der aktuellen Rechtslage machbar ist. Eine gesetzliche Grundlage wäre jedoch für die Rechtssicherheit in der Umsetzung und die Zielerreichung vorteilhaft.

6. Danksagung

Das Projekt wird von der Arbeitsgruppe Rechtsinformatik, Juridicum, Universität Wien, unter der Leitung von Prof. Dr. Dr. Erich Schweighofer durchgeführt. Die Autoren danken für die wesentliche Unterstützung und wichtige Hinweise.

[34] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Resilienz kritischer Einrichtungen, COM(2020) 829 final.

[35] Art. 9 Abs. 1 leg. cit.: „*Die Mitgliedstaaten unterstützen kritische Einrichtungen bei der Verbesserung ihrer Resilienz. [...]*“.

[36] Siehe oben, Abschnitt 2.

[37] Siehe ausdrücklich in Erw. 19 i.V.m. Art. 9 COM(2020) 829 final.