27.03.2026

Expertenpapier zur Überprüfung von Transparenzpflichten im Kontext des Schutzes kritischer Infrastrukturen

Die gesetzlichen Regelungen enthalten eine Vielzahl an Transparenzpflichten, nach denen Infrastrukturbetreiber und mit Infrastrukturen befasste Behörden Informationen zu veröffentlichen oder auf Anfrage herauszugeben haben. Die Transparenzpflichten basieren häufig auf EU-Recht bzw. auf seit Jahrzehnten bestehenden Regelungen. Hierbei ist neben einer Zunahme an gesetzlichen Regelungen, die der Transparenz dienen sollen, in den letzten Jahren insbesondere auch in der Behördenpraxis ein Anstieg an von Vorhabenträgern geforderten Informationen zu verzeichnen.

So ergeben sich beispielsweise im Rahmen von Genehmigungsverfahren aus diversen Gesetzen Pflichten zur Veröffentlichung der Antragsunterlagen sowie der Genehmigungen. Diese Unterlagen haben mittlerweile einen sehr hohen Detailgrad. Obwohl Transparenz gegenüber der Öffentlichkeit und gegenüber den Marktteilnehmern grundsätzlich zu begrüßen ist und im Einzelfall auch zu mehr Akzeptanz führen kann, ermöglicht diese auf der anderen Seite auch jedem Dritten, sich ein umfangreiches Bild über Details des Infrastruktursystems zu verschaffen und damit auch besonders „attraktive“ Ziele für Sabotage ohne viel Aufwand zu erkennen. Aus den veröffentlichten Informationen sind nicht nur einzelne Standorte und die genaue Lage und Gestalt technischer Anlagen erkennbar, sondern auch Lastflüsse und Knotenpunkte. Zudem lassen sich durch diese veröffentlichten Informationen sonstige technische Zusammenhänge einfacher identifizieren. Dadurch wird für jeden prognostizierbar, an welcher Stelle im Übertragungsnetz ein möglichst hoher Schaden verursacht werden kann.

Vor diesem Hintergrund wird angeregt, die Regelungen zu Transparenz- und Informationspflichten zu prüfen und, falls möglich, einzuschränken. Es sollten Möglichkeiten geschaffen werden, bestimmte Informationen mit Verweis auf die öffentliche Sicherheit zurückhalten zu können.

1. Anpassungen im Vergaberecht

Die vergaberechtlichen Transparenz- und Veröffentlichungspflichten aus §§ 97 ff. GWB, VgV sowie §§ 19 ff. EEG verlangen, soweit dies für die jeweiligen ÜNB anwendbar ist, dass bei Ausschreibungen Informationen zu Projekten, Standorten und technischen Anforderungen offengelegt werden. Gleichzeitig können aus diesen Unterlagen sicherheitsrelevante Schwachstellen abgeleitet werden. Eine Lösung besteht darin, KRITIS Betreiber weiterhin dem Vergaberecht zu unterwerfen, dieses jedoch für sicherheitskritische Beschaffungen einschränkend anzuwenden: z.B. Herausgabe der vollständigen Vergabeunterlagen nur an Bieter, deren Eignung bereits geprüft wurde oder Schaffung eines zusätzlichen Ausnahmetatbestandes für ein Verhandlungsverfahren ohne Teilnahmewettbewerb in § 13 Abs. 2 SektVO mit beschränktem Bieterkreis. So bleiben Dokumentations- und Wirtschaftlichkeitsanforderungen bestehen, während sicherheitsrelevante Inhalte von Ausschreibungsunterlagen nicht öffentlich zugänglich gemacht werden bzw. nur befugten Bietern kontrolliert bereitgestellt werden.

2. Transparenzpflichten aus dem Energiewirtschaftsgesetz (EnWG)

- *§§ 111d-111g EnWG; §15 MaStRV*

Die von der BNetzA nach diesen Regelungen betriebenen Plattformen wie die nationale Informationsplattform (SMARD); das Marktstammdatenregister oder die nationale Transparenzplattform enthalten u.a. öffentlich zugängliche Stamm- und Bewegungsdaten zu den Medien Elektrizität, Gas und Wasserstoff.

§ 111d Abs. 2 Satz 5 EnWG und § 111g Abs. 2 Satz 9 EnWG statuieren diesbezüglich bereits, dass die Bundesnetzagentur Daten, die geeignet sind, die Sicherheit oder Zuverlässigkeit des Elektrizitätsversorgungssystems oder die Sicherheit und Ordnung zu gefährden, oder die europäischen kritischen Anlagen betreffen, nur im Einvernehmen mit den Betreibern der Übertragungsnetze veröffentlichen darf. Auch die Normen zum Marktstammdatenregister regeln, dass das Marktstammdatenregister unter Berücksichtigung der einschlägigen Standards und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik zu erfolgen hat, vgl. § 111e Abs. 3 Nr. 2b) EnWG, und dass durch Rechtsverordnung Art und Umfang der Veröffentlichungen unter Beachtung der Anforderungen an die Sicherheit und Zuverlässigkeit des Energieversorgungssystems näher ausgestaltet werden können, vgl. § 111f Nr. 9 EnWG.

Es sollte insofern überprüft werden, ob diese Daten in der heutigen hohen Auflösung tatsächlich allgemein zugänglich sein müssen und ob der Zugang in seiner heutigen Form nur bei nachgewiesenem berechtigtem Interesse möglich sein sollte. Ziel sollte es sein, dass Ausnahmemöglichkeiten beim Datenzugang ausreichend Sicherheit schaffen bzw. wie eine konsequentere Nutzung der Ausnahmen sichergestellt werden kann.

- *§ 23c EnWG sowie § 12b EnWG*

Es besteht die gesetzliche Verpflichtung zur Veröffentlichung von Netzkarten, Engpässen, Baumaßnahmen etc. über den Netzausbauplan, der alle 2 Jahre zu aktualisieren ist. Über diese Veröffentlichung werden Netzknoten und stark belastete Betriebsmittel transparent gemacht. Beides sind sensible Punkte in der Energieversorgung. Potenziell kritische Daten sind auch mit der Erstellung des Netzentwicklungsplans durch die Betreiber von Übertragungsnetzen gemäß § 12b EnWG verbunden.

Es sollte daher überprüft werden, inwiefern solche Daten grundsätzlich minimiert bzw. der Zugang zu solchen Daten eingeschränkt werden müsste.

3. Anpassungen der Regulierungsvorschriften des Informationsfreiheitsgesetzes (IFG)

Allgemeine Regulierungsvorschriften, insbesondere das Informationsfreiheitsgesetz sowie §§ 8 und 9 UIG und die entsprechenden Landesregelungen, müssen so ausgestaltet werden, dass sicherheitsrelevante Informationen ausgenommen werden können. Da Auskunftspflichten nach IFG und Landesgesetzen sektorübergreifend bestehen und auf Antrag Einsicht ermöglichen, besteht das Risiko, dass sensible Daten veröffentlicht werden. Daher ist eine Anpassung der Ablehnungsgründe in § 6 IFG erforderlich, um sicherheitsrelevante Inhalte auszuschließen. Zweckmäßig erscheint es, in einem zentralen Regelwerk – etwa im KRITISDachgesetz – eine allgemeine, gesetzlich verankerte Beschreibung sicherheitsrelevanter Sachverhalte aufzunehmen, auf die in den einschlägigen Fachgesetzen (insbesondere VwVfG, EnWG, NABEG, BImSchG sowie IFG) ausdrücklich verwiesen werden kann. In der Praxis zeigt sich, dass für die rechtsanwendenden Stellen regelmäßig nicht hinreichend klar ist, nach welchen Kriterien und anhand welcher Maßstäbe im konkreten Einzelfall eine Sicherheitsrelevanz substantiiert zu begründen ist. Gerade diese Unsicherheit führt dazu, dass die bestehenden gesetzlichen Instrumente nicht durchgängig ausgeschöpft werden können. Würden entsprechende, hinreichend konkretisierte Maßstäbe zur Begründung der Sicherheitsrelevanz normativ vorgegeben, könnte der notwendige Schutz bereits auf Grundlage des geltenden Rechts gewährleistet werden; eines zusätzlichen Regelungsregimes bedürfte es insoweit nicht zwingend.

Die gesetzlichen Regelungen (Umweltinformationsgesetz (UIG), Informationsfreiheitsgesetz (IFG) des Bundes und der Länder sowie Geodatenzugangsgesetz (GeoZG)) sehen dabei grundsätzlich einen weiten Anwendungsbereich vor. Die Gesetze beinhalten jeweils auch Regelungen zum Schutz öffentlicher und/ oder sonstiger Belange. **Hier sollte geprüft werden, ob es eine Stärkung oder Ausweitung der Ablehnungsgründe in Bezug auf KRITIS geben sollte. Insbesondere eine Subsumption von KRITIS unter das Schutzgut der öffentlichen Sicherheit wäre hilfreich.**

Es wird angeregt, in § 8 die Sätze 3 und 4 (NEU) UIG zu ergänzen:

„Kritische Infrastrukturen gemäß § 2 Absatz 10 BSIG in Verbindung mit der Verordnung nach § 10 Absatz 1 BSIG dienen dem Schutz bedeutsamer Schutzgüter der öffentlichen Sicherheit im Sinne von Nummer 1. Das Informationsinteresse des Antragstellers sowie das öffentliche Interesse an der Bekanntgabe überwiegen bei Informationen, die diese kritischen Infrastrukturen betreffen, in der Regel nicht das Geheimhaltungsinteresse.“

4. **Öffentlichkeit bei Gerichtsverfahren**

Konsequent wäre die Möglichkeit, bei Klagen, die z.B. die Genehmigung von KRITIS zum Inhalt haben, die Öffentlichkeit auszuschließen soweit die Gefahr besteht, dass ansonsten sicherheitsrelevante Informationen nach außen dringen. Ein Ansatzpunkt hierfür wäre § 172 GVG (anwendbar gemäß § 55 VwGO), der es dem Gericht ermöglicht, unter bestimmten Umständen die Öffentlichkeit für die Verhandlung oder einen Teil davon auszuschließen. **Es wäre zu prüfen, ob sicherheitsrelevante Informationen zu KRITIS bereits unter den Ausnahmetatbestand des § 172 Nr. 1 GVG fallen oder ob eine Ergänzung zielführend wäre.**

5. **Überprüfung der Transparenzpflichten und Vermeidung neuer Transparenzvorgaben durch EU Sicherheits- und Resilienzvorgaben**

Transparente Prozesse sind in vielerlei Hinsicht berechtigt. Unter der Zielstellung der Gefahrenvorsorge gilt es jedoch, bestehende Transparenzpflichten systematisch einer Überprüfung zu unterziehen. Die Veröffentlichungen gemäß der EU VO543/2013, Artikel 10 sind hier zu nennen, da mit konkreter Leitungsbezeichnung ersichtlich wird, in welchen Regionen Leitungen bereits abgeschaltet sind oder werden. Hierdurch lassen sich Rückschlüsse auf Areale ziehen, in denen Netzelemente besonders beansprucht sind.

Die Richtlinien (EU) 2022/2555 (NIS2) und 2022/2557 (CER) verlangen Vorgaben für kritische Einrichtungen, bergen jedoch das Risiko, dass durch öffentliche Offenlegung von Resilienz- und Risikoanalysen sensible Schutzkonzepte sowie präzise Standort- oder Asset-Daten bekannt werden.

Vor diesem Hintergrund besteht ein Prüfauftrag, bestehende und künftige Transparenz- und Veröffentlichungspflichten systematisch daraufhin zu überprüfen, ob sie sicherheitsrelevante Informationen in unangemessener Detailtiefe öffentlich zugänglich machen. Ziel sollte sein, dass sensible Informationen – insbesondere zu Standorten, Netzelementen und Resilienzbewertungen – primär gegenüber zuständigen Behörden offengelegt werden. Öffentliche Berichte sollten demgegenüber nur in stark abstrahierter Form erfolgen. Detaillierte Geodaten, konkrete Standortangaben sowie Resilienz- und Schutzinformationen sollten im CER-Kontext grundsätzlich nicht veröffentlicht werden. Soweit Geodaten erforderlich sind, sollten diese ausschließlich anonymisiert oder gerastert bereitgestellt werden.

6. **Unkenntlichmachung sicherheitsrelevanter KRITIS-Daten in öffentlichen Karten- und Mapping-Diensten**

Zur Stärkung des Schutzes kritischer Energieinfrastrukturen sollte geprüft werden, sicherheitsrelevante Assets und Lagerstandorte aus öffentlich zugänglichen Kartendiensten zu verpixeln oder zu entfernen sowie den Zugang zu spezialisierten Infrastruktur-MappingTools- wie der Open Infrastructure Map auf Behörden und Netzbetreiber zu begrenzen.