FNB Gas - Stellungnahme

zum Entwurf eines Gesetzes zur Anpassung von Transparenz-, Veröffentlichungs- und Informationspflichten zum angemessenen Schutz kritischer Infrastruktur

Berlin, 17.11.2026

Über FNB Gas:

FNB Gas e.V. ist der Zusammenschluss der überregionalen deutschen Fernleitungsnetzbetreiber mit Sitz in Berlin. Seine Mitglieder betreiben zusammen ein rund 40.000 Kilometer langes Leitungsnetz für den Transport von Erdgas und errichten gemeinsam das rund 9.000 Kilometer lange Wasserstoff-Kernnetz. Die 2012 gegründete Vereinigung unterstützt ihre Mitglieder bei der Erfüllung ihrer gesetzlichen und regulatorischen Verpflichtungen. Zudem koordiniert sie die integrierte Netzentwicklungsplanung für Gas und Wasserstoff auf der Transportnetzebene. Darüber hinaus tritt die Vereinigung für die aktive Förderung eines sicheren und effizienten Betriebs der Gastransportinfrastruktur sowie für ihre kontinuierliche Weiterentwicklung an die Bedarfe des zukünftigen Energiesystems ein.

Mitglieder der Vereinigung sind die Unternehmen bayernets GmbH, Ferngas Netzgesellschaft mbH, Fluxys TENP GmbH, GASCADE Gastransport GmbH, Gastransport Nord GmbH, Gasunie Deutschland Transport Services GmbH, NaTran Deutschland GmbH, Nowega GmbH, ONTRAS Gastransport GmbH, Open Grid Europe GmbH, terranets bw GmbH und Thyssengas GmbH.

Einleitung

Angesichts der veränderten sicherheitspolitischen Rahmenbedingungen und der gestiegenen Bedrohungslage ist eine Überprüfung bestehender Transparenzanforderungen geboten. Der Gesetzentwurf greift damit ein zentrales Anliegen der Betreiber kritischer Infrastrukturen auf und leistet einen wichtigen Beitrag zur Stärkung von Resilienz und Versorgungssicherheit.

Betreiber kritischer Infrastrukturen sind derzeit verpflichtet, über Transparenzplattformen, Planfeststellungs- und Netzentwicklungsverfahren sowie den Infrastrukturatlas umfangreiche Informationen über ihre Infrastrukturen bereitzustellen. Hierzu zählen unter anderem Angaben zu Anlagenstandorten, Leitungsverläufen, Kapazitäten und Betriebsdaten. Solche Informationen können Rückschlüsse auf kritische Infrastrukturen und deren Verwundbarkeiten ermöglichen und damit das Risiko gezielter Sabotageakte erhöhen. Mit der fortschreitenden Digitalisierung und den zunehmenden Möglichkeiten der Datenverarbeitung können Informationen aus unterschiedlichen Quellen immer einfacher zusammengeführt und ausgewertet werden. Dies verstärkt die beschriebenen Risiken zusätzlich.

FNB Gas begrüßt daher ausdrücklich den im Gesetzentwurf verfolgten Ansatz, den Schutz kritischer Infrastrukturen bei der Ausgestaltung von Transparenz-, Veröffentlichungs- und Informationspflichten stärker zu berücksichtigen und bestehenden Schutzlücken entgegenzuwirken. Insbesondere die vorgesehenen Regelungen zum Schutz sicherheitsrelevanter Informationen im Informationsfreiheitsgesetz stellen einen wichtigen Schritt zur Verbesserung des Schutzes von Elektrizitäts-, Gas- und Wasserstoffversorgungssystemen dar.

Aus Sicht der Fernleitungsnetzbetreiber (FNB) besteht bei den im vorliegenden Referentenentwurf vorgesehenen Änderungen jedoch in einzelnen Bereichen weiterer Konkretisierungs- und Anpassungsbedarf. Dies betrifft insbesondere die Bestimmung schutzbedürftiger Informationskategorien, die Einbindung der betroffenen Netzbetreiber bei der Sicherheitsbewertung von Veröffentlichungen, den Schutz sicherheitsrelevanter Informationen bereits im Genehmigungsverfahren sowie den Umgang mit sensiblen Infrastrukturdaten im Infrastrukturatlas.

Zu den Regelungen des Gesetzesentwurfs im Einzelnen

Artikel 1 Nr. 2 zu § 111g Absatz 2 Satz 9 EnWG

Die vorgeschlagene Anpassung in § 111g Abs. 2 S. 9 EnWG würde dazu führen, dass die Bundesnetzagentur (BNetzA) auf der neuen nationalen Transparenzplattform Daten, die

a) geeignet sind, die Sicherheit oder Zuverlässigkeit der Elektrizitäts-, Gas- oder Wasserstoffversorgungssysteme zu gefährden

b) geeignet sind, die Sicherheit und Ordnung zu gefährden

c) europäische kritische Anlagen betreffen

nicht veröffentlichen darf.

Aus dieser vorgeschlagenen Regelung geht nicht eindeutig hervor, welche Daten von der BNetzA veröffentlicht werden dürfen bzw. nicht veröffentlicht werden dürfen. Unseres Erachtens würden die Regelungen im Gesetzesentwurf die Entscheidung über die Veröffentlichung sicherheitsrelevanter Informationen auf die Ebene der behördlichen Einzelfallbewertung durch die BNetzA verlagern.

Ob Stamm-, Geo- oder Bewegungsdaten einer bestimmten Datenart im Marktstammdatenregister (oder einer anderen BNetzA-Plattform) veröffentlicht werden bzw. nicht veröffentlicht werden, würde faktisch im Ermessen der BNetzA liegen. Die von der BNetzA betriebenen Plattformen Marktstammdatenregister (§§ 111e und 111f EnWG), SMARD (§ 111d EnWG) und zukünftig nationale Transparenzplattform (§ 111g EnWG)) enthalten öffentlich zugängliche Stamm- und Bewegungsdaten. Aufgrund der geplanten Schnittstelle(n) zwischen Marktstammdatenregister einerseits (Stamm-/Geodaten zu Anlagen der Medien Strom, Gas und Wasserstoff) und SMARD andererseits (Bewegungsdaten zu den Medien Strom, Gas und Wasserstoff) können Stamm-/Geodaten aus dem Marktstammdatenregister und Bewegungsdaten aus SMARD problemlos zusammengetragen, kombiniert, aufbereitet und ausgewertet werden.

Die Beurteilung, ob bestimmte Informationen Rückschlüsse auf die Sicherheit, Integrität oder Resilienz eines Versorgungssystems ermöglichen, setzt regelmäßig detaillierte Kenntnisse des Netzes, der betrieblichen Abläufe, der bestehenden Redundanzkonzepte sowie der konkreten Schutzmaßnahmen voraus. Diese Kenntnisse liegen naturgemäß in erster Linie beim jeweiligen Netzbetreiber vor, weshalb eine Beurteilung durch die Regulierungsbehörde allein nicht sachgerecht ist. Daher regen wir an, dass die Sicherheitsbewertung im Einvernehmen der BNetzA mit dem jeweiligen Netzbetreiber erfolgen sollte.

Wir schlagen daher vor, die Regelung in § 111g Abs. 2 S. 9 EnWG wie folgt zu ergänzen:

„Die Bundesnetzagentur darf Daten, die geeignet sind, die Sicherheit oder Zuverlässigkeit der Elektrizitäts-, Gas- oder Wasserstoffversorgungssysteme oder die Sicherheit und Ordnung zu gefährden, oder die europäische kritische Anlagen betreffen, nicht veröffentlichen ***und stellt über die sicherheitsgefährdende Eigenschaft von Daten vor Veröffentlichung das Einvernehmen mit den jeweiligen Betreiber des Elektrizitäts-, Gas- oder Wasserstoffversorgungssystems her***; Absatz 1 Satz 1 bleibt hiervon unberührt."

Artikel 2 Änderung des Informationsfreiheitsgesetzes

Im Referentenentwurf ist in Art. 2 vorgesehen, im Informationsfreiheitsgesetz (IFG) in § 3 eine neue Nr. 9 mit folgendem Wortlaut anzufügen: „hinsichtlich Infrastrukturen, die durch Rechtsvorschrift als kritische Infrastrukturen bestimmt worden sind oder die besonders schutzbedürftig zur Wahrung der öffentlichen Sicherheit sind."

Der FNB Gas begrüßt den Vorschlag grundsätzlich, denn diese Regelung dient dem Schutz der Elektrizitäts-, Gas- oder Wasserstoffversorgungssysteme. Allerdings sollten in die Gesetzesbegründung für die Anwendung typische schutzbedürftige Informationskategorien und belastbare Kriterien aufgenommen werden. Für Elektrizitäts-, Gas- oder Wasserstoffversorgungssysteme würden dazu insbesondere sicherheitsrelevante Angaben zu Standorten und Trassen, technischer Auslegung, Kapazitäten, Verwundbarkeiten und Schutzvorkehrungen gehören.

Fokus auf Schutz von Informationen bereits im Genehmigungsverfahren

Der Gesetzentwurf berücksichtigt bislang nicht hinreichend, dass kritische Infrastruktur bereits in der Genehmigungsphase schutzwürdig sein kann. Mit dem Aufbau des Wasserstoffkernnetzes werden bundesweit neue Leitungs- und Anlagenstrukturen geschaffen, deren Lage und technische Ausgestaltung regelmäßig Gegenstand von Planfeststellungsverfahren nach den §§ 43 ff. EnWG sind. Vor dem Hintergrund der vorgesehenen digitalen Veröffentlichung von Verfahrensunterlagen sollte der Gesetzgeber ausdrücklich sicherstellen, dass sicherheitsrelevante Informationen auch im Rahmen dieser Verfahren einem

angemessenen Schutz unterliegen. Der Schutz kritischer Energieinfrastruktur muss bereits im Genehmigungsverfahren ansetzen und darf nicht erst mit der Inbetriebnahme der jeweiligen Anlage beginnen.

Schutz sensibler Infrastrukturdaten im Infrastrukturatlas – Anpassung des Telekommunikationsgesetzes (TKG)

Der mit dem Gesetzentwurf verfolgte Schutz kritischer Energieinfrastruktur muss auch bei der Bereitstellung von Daten im Infrastrukturatlas (ISA) der BNetzA konsequent gewährleistet werden. FNB übermitteln nach §§ 78, 79 TKG Informationen über ihre zu Telekommunikationszwecken nutzbaren Infrastrukturen, darunter Lichtwellenleitertrassen, die insbesondere der internen Datenübertragung und Netzsteuerung dienen. Da diese vielfach parallel zu Gasversorgungsleitungen verlaufen, ermöglichen ihre Geodaten Rückschlüsse auf die Lage kritischer Gasinfrastruktur. Der ISA ist zwar nicht öffentlich zugänglich; trotz der bestehenden Zugangsbeschränkungen verbleibt jedoch ein Risiko unbefugter Datenweitergabe und damit einer Gefährdung der Versorgungssicherheit.

Der FNB Gas fordert daher, im Zuge des Anpassungsgesetzes auch den Schutz sensibler Infrastrukturdaten nach dem TKG rechtssicher auszugestalten. Hier müssten entweder kritische Energieinfrastrukturen vom Veröffentlichungsgebot nach dem TKG schon tatbestandlich ausgenommen werden. Oder es müssten die vorhandenen Ausnahmen von der Aufnahme in den ISA nach § 79 Abs. 3 Satz 1 Nr. 1 und 3 TKG behördlich konsistent angewendet werden, um die Schutzbedürftigkeit der gesamten Energieinfrastruktur (Strom, Gas und Wasserstoff) einschließlich der für ihren sicheren Betrieb erforderlichen Telekommunikationsinfrastruktur wirksam zu erfassen. Denn bis dato ist die behördliche Praxis insoweit inkonsistent und gewährt den ÜNB Ausnahmen, den FNB jedoch nicht.

Zu diesem Zwecke sollte gesetzlich klargestellt werden, dass auch mittelbare Rückschlüsse auf schutzbedürftige Energieinfrastruktur zu berücksichtigen sind und die Prüfung nicht auf Gefahren für die Telekommunikationsnutzung beschränkt werden darf. Sicherheitsrelevante Trassendaten sind bei entsprechenden Gefährdungen von der Aufnahme in den ISA auszunehmen. Die Sicherheitsbewertung sollte im Einvernehmen mit dem betroffenen Netzbetreiber erfolgen. So wird verhindert, dass der mit dem Gesetzentwurf angestrebte Informationsschutz durch die Bereitstellung derselben oder vergleichbar sensibler Daten über andere behördliche Plattformen unterlaufen wird.

Weitere Anpassungen

Zusätzlich sind aus Sicht der FNB weitere Anpassungen in den §§ 111e bis 111g EnWG sowie in verschiedenen weiteren Gesetzen erforderlich, um den Schutz der kritischen Infrastruktur sicherstellen zu können. Hierzu verweisen wir auf unsere an das Bundesministerium für Wirtschaft und Energie versendete Stellungnahme vom 20.11.2025 (*Stellungnahme-Gutachten-SG2602190026.pdf*)