TenneT Positionspapier Überprüfung Transparenzpflichten

Zusammenfassung

Vor dem Hintergrund der gestiegenen Bedrohungslage für kritische Infrastrukturen ist eine Neubewertung bestehender Transparenzpflichten gemeinsam mit Behörden erforderlich. Aus Sicht der TenneT sollten zentrale Veröffentlichungspflichten entsprechend überarbeitet werden.
Im Vergabe- und Planungsrecht sowie im Informationsfreiheitsrecht müssen sicherheitsrelevante technische Details künftig stärker geschützt werden. EU-Vorgaben zu Sicherheit und Resilienz dürfen keine neue Offenlegung sensibler Standort- oder Schutzkonzepte verlangen, solche Informationen sollten ausschließlich Behörden zugänglich sein.

1. Anpassungen im Vergaberecht

Die vergaberechtlichen Transparenz- und Veröffentlichungspflichten aus §§ 97 ff. GWB, VgV sowie §§ 19 ff. EEG verlangen, dass bei Ausschreibungen Informationen zu Projekten, Standorten und technischen Anforderungen offengelegt werden. Gleichzeitig könnten aus diesen Unterlagen sicherheitsrelevante Schwachstellen abgeleitet werden. Eine Lösung besteht darin, KRITIS Betreiber weiterhin dem Vergaberecht zu unterwerfen, jedoch für sicherheitskritische Beschaffungen Sonderregelungen z.B. analog zu dem abgestuften System im Verteidigungs- und Sicherheitsbereich zum Schutz von Sicherheitsinteressen und den Sonderregelungen der VSVgV anzuwenden. So bleiben Dokumentations- und Wirtschaftlichkeitsanforderungen bestehen, während sicherheitsrelevante Inhalte von Ausschreibungsunterlagen nicht öffentlich zugänglich gemacht werden bzw. nur befugten Bietern kontrolliert bereitgestellt werden.

2. Anpassungen im Planungsrecht: BImSchG

Im Planungsrecht nach BImSchG sollte die Auslegungspflicht auf Unterlagen mit Relevanz für die Öffentlichkeit beschränkt werden, etwa Emissions- /Immissionsberichte oder UVP-Berichte, nicht jedoch für detaillierte technische Unterlagen gelten. Da im Verfahren nach § 10 der 9. BImSchV Planungsunterlagen sektorübergreifend online bereitgestellt werden, besteht das Risiko, dass sensible Daten öffentlich zugänglich sind. Daher ist das Schutzniveau zu erhöhen, indem sicherheitsrelevante Informationen wie Betriebsgeheimnisse behandelt werden.

3. Anpassungen Regulierungsvorschriften: Informationsfreiheitsgesetz

Allgemeinen Regulierungsvorschriften, insbesondere das Informationsfreiheitsgesetz sowie §§ 8 und 9 UIG und die entsprechenden Landesregelungen, müssen so ausgestaltet bleiben, 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.

4. Keine neuen Transparenzvorgaben durch EU Sicherheits- und Resilienzvorgaben

Die Richtlinien (EU) 2022/2555 (NIS2) und 2022/2557 (CER) verlangen Vorgaben für kritische Einrichtungen, bergen jedoch auch das Risiko, dass durch öffentliche Offenlegung von Resilienz- und Risikoanalysen sensible Schutzkonzepte sowie präzise Standort- oder Asset-Daten bekannt werden. Da durch Kombination offener Datensätze Re-Identifikation und Standortschutzrisiken entstehen, müssen diese Informationen primär nur gegenüber Behörden offengelegt werden. Öffentliche Berichte dürfen nur in stark abstrahierter Form erscheinen, ohne detaillierte Geodaten. Standort- und Resilienzangaben sollen im CER-Bereich nicht zu veröffentlichen sein. Geodaten sollten lediglich anonymisiert oder gerastert bereitgestellt und Schutzkonzepte ausschließlich intern bzw. behördlich behandelt werden.

Generell betrachten wir zentralisierte Datensammlungen auch aus Sicherheitsgründen kritisch und sprechen uns dafür aus, künftige europäische und nationale Gesetzesvorhaben frühzeitig dahingehend zu prüfen, ob entsprechende Transparenzanforderungen wirklich notwendig und sicher realisierbar sind.