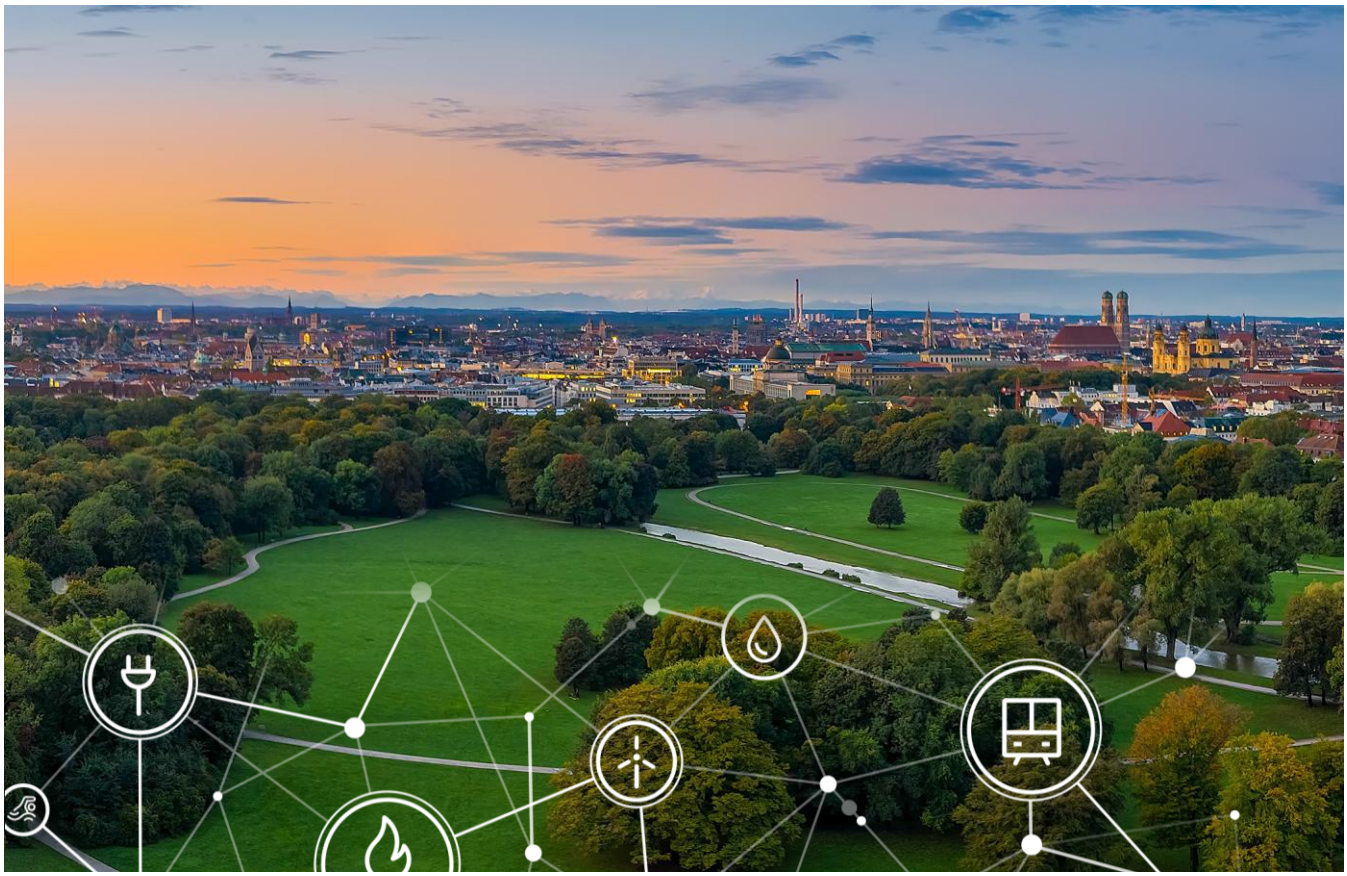
Stadtwerke München



Stellungnahme der Stadtwerke München zum Referentenentwurf für ein Gesetz zur Anpassung von Transparenz-, Veröffentlichungs- und Informationspflichten zum angemessenen Schutz kritischer Infrastrukturen

Lobbyregisternummer (national): R000611

Inhalt

I. Einleitung 3
II. Forderungen der Stadtwerke München 3
1. Einheitlichen KRITIS-Schutzvorbehalt im EnWG verankern 3
2. Schutz über den gesamten Datenlebenszyklus gewährleisten 4
3. Bereits veröffentlichte Infrastrukturdaten überprüfen und erforderlichenfalls entfernen 4
4. Detailtiefe von Netzausbau- und Netzentwicklungsplänen reduzieren 4
5. Veröffentlichung von Netzstrukturdaten nach § 23c EnWG begrenzen 5
6. Sicherheitsrelevante Redispatch-, Engpass- und Systemführungsdaten schützen 5
7. Schutz kritischer Anlagen im Marktstammdatenregister stärken 6
8. Nationale Transparenzplattformen auf Erforderlichkeit und Datenumfang überprüfen ... 6
9. Schutz in Planungs-, Genehmigungs- und Beteiligungsverfahren stärken 7
10. Sicherheitsrelevante Infrastrukturinformationen in Vergabeverfahren schützen 7
11. Sektorübergreifenden Schutz kommunaler Infrastrukturen sicherstellen 7
12. Europäischen Rechtsrahmen einbeziehen 8
III. Zusammenfassung 8

I. Einleitung

Die Stadtwerke München GmbH (SWM) begrüßen die mit dem Referentenentwurf verfolgte Zielsetzung, bestehende Transparenz-, Veröffentlichungs- und Informationspflichten mit Blick auf den Schutz kritischer Infrastrukturen zu überprüfen und erforderlichenfalls anzupassen.

Öffentlich zugängliche Informationen über kritische Infrastrukturen können Ausspähung, Sabotage oder Anschläge erleichtern. Besonders relevant ist, dass auch Informationen, die isoliert betrachtet wenig sicherheitskritisch erscheinen, in ihrer Zusammenschau Rückschlüsse auf Lage, Auslegung, Kapazitäten oder Verwundbarkeiten kritischer Infrastrukturen ermöglichen können. Dieser im Referentenentwurf verankerte Schutzgedanke entspricht den praktischen Erfahrungen eines Betreibers kritischer Infrastrukturen.

Die vorgesehenen Änderungen der §§ 12f und 111g EnWG sind daher grundsätzlich zu begrüßen. Insbesondere stärken der Ausschluss sicherheitsrelevanter Daten von der Herausgabe nach § 12f Abs. 2 EnWG und das Veröffentlichungsverbot nach § 111g Abs. 2 Satz 9 EnWG den Schutz sensibler energiewirtschaftlicher Informationen.

Der Entwurf ist aus SWM-Sicht ein wichtiger erster Schritt, aber noch kein umfassendes Transparenzanpassungsgesetz für kritische Infrastrukturen. Weitere sicherheitsrelevante Transparenz- und Veröffentlichungspflichten werden bislang nicht adressiert. Entscheidend ist daher, den eingeschlagenen Ansatz konsequent fortzuführen und den Schutz kritischer Infrastrukturen auch in weiteren einschlägigen Fachgesetzen zu verankern.

Vor diesem Hintergrund benennen die SWM im Folgenden konkrete Anpassungsbedarfe und Forderungen zum Schutz sicherheitsrelevanter Informationen in der Energieversorgung sowie in weiteren Bereichen der kommunalen Daseinsvorsorge.

II. Forderungen der Stadtwerke München

1. Einheitlichen KRITIS-Schutzvorbehalt im EnWG verankern

Der Referentenentwurf passt mit den §§ 12f und 111g EnWG bislang lediglich einzelne Vorschriften an. Sicherheitsrelevante Informations-, Transparenz- und Veröffentlichungspflichten finden sich jedoch an zahlreichen weiteren Stellen des EnWG und der auf seiner Grundlage erlassenen Rechtsverordnungen. Eine ausschließlich punktuelle Anpassung birgt die Gefahr fortbestehender Schutzlücken und unterschiedlicher Schutzmaßstäbe.

SWM-Forderung: Ergänzend zu den vorgesehenen Einzeländerungen sollte im EnWG ein übergreifender Schutzvorbehalt für sämtliche gesetzlichen Informations-, Transparenz-, Datenbereitstellungs- und Veröffentlichungspflichten verankert werden. Sicherheitsrelevante Informationen dürfen danach nicht veröffentlicht oder allgemein zugänglich gemacht werden, wenn sie allein oder in Verbindung mit anderen zugänglichen Informationen geeignet sind, die Sicherheit oder Zuverlässigkeit von Energieversorgungsnetzen oder Energieanlagen zu gefährden oder Rückschlüsse auf kritische Anlagen, neuralgische Netzpunkte, Redundanzen, Engpasssituationen oder strukturelle Verwundbarkeiten zu ermöglichen. Der Schutzvorbehalt sollte Elektrizitäts-, Gas-, Wasserstoff- und Wärmeinfrastrukturen sowie die hierfür erforderlichen Informations- und Kommunikationstechnologien erfassen. Aggregierte, abstrahierte, kategorisierte oder anonymisierte Angaben müssen Vorrang vor der Offenlegung detaillierter Informationen haben.

2. Schutz über den gesamten Datenlebenszyklus gewährleisten

Der Schutz kritischer Infrastrukturen darf nicht erst bei der Veröffentlichung sicherheitsrelevanter Informationen einsetzen. Bereits ihre Erhebung, Übermittlung, Zusammenführung und zentrale Speicherung können zusätzliche Risiken schaffen. Dies gilt insbesondere für Datenbestände, die Informationen verschiedener Unternehmen, Infrastruktursektoren oder Verwaltungsebenen verbinden und dadurch ein sektorübergreifendes Lagebild ermöglichen. Zusätzliche Risiken entstehen durch die Einbindung externer Planungsbüros, Gutachter, IT-Dienstleister und Unterauftragnehmer.

SWM-Forderung: Für sicherheitsrelevante Infrastrukturdaten sind verbindliche Vorgaben zur Datenminimierung, Zweckbindung, sicheren Übermittlung, Speicherung, Zugriffssteuerung und Löschung festzulegen. Detaillierte Daten dürfen nur verlangt werden, wenn der gesetzliche Zweck nicht mit aggregierten, abstrahierten oder anonymisierten Angaben erreicht werden kann. Erforderlich sind insbesondere gesicherte Übermittlungswege, rollenbasierte Berechtigungen, Zwei-Faktor-Authentifizierung, regelmäßige Berechtigungskontrollen und eine Protokollierung von Zugriffen und Datenexporten. Für externe Dienstleister und deren Unterauftragnehmer müssen dieselben Anforderungen gelten. Mehrfacherhebungen, parallele Datenbestände und eine Speicherung über den erforderlichen Zeitraum hinaus sind zu vermeiden.

3. Bereits veröffentlichte Infrastrukturdaten überprüfen und erforderlichenfalls entfernen

Ein wirksamer Schutz kritischer Infrastrukturen darf sich nicht auf künftige Veröffentlichungen beschränken. Zahlreiche sicherheitsrelevante Informationen sind bereits auf Internetseiten, in Registern, Planungsunterlagen, Datenportalen und Archiven öffentlich verfügbar. Durch verbesserte Möglichkeiten zur automatisierten Recherche, Verknüpfung und Auswertung kann sich die Sicherheitsrelevanz auch älterer Datenbestände nachträglich erhöhen.

SWM-Forderung: Bund, Länder und zuständige Behörden sollten verpflichtet werden, bestehende Veröffentlichungen und öffentlich zugängliche Datenbestände regelmäßig auf ihre aktuelle Sicherheitsrelevanz zu überprüfen. Ergibt die Prüfung, dass Informationen allein oder in Verbindung mit weiteren Datenquellen ein Sicherheitsrisiko begründen, müssen sie nachträglich entfernt, anonymisiert, aggregiert oder in ihrer Detailtiefe reduziert werden können. Betreiber kritischer oder besonders schutzbedürftiger Infrastrukturen sollten ein gesetzlich geregeltes Verfahren erhalten, mit dem sie die Überprüfung und erforderlichenfalls die Entfernung sicherheitsrelevanter Informationen beantragen können.

4. Detailtiefe von Netzausbau- und Netzentwicklungsplänen reduzieren

Netzausbaupläne der Verteilernetzbetreiber nach § 14d EnWG und die zugrunde liegenden Regionalszenarien können Rückschlüsse auf lokale Engpässe, Trassenverläufe, Auslastungen und konkrete Optimierungsmaßnahmen ermöglichen. Auch **Netzentwicklungspläne für Strom nach §§ 12a und 12b EnWG sowie für Gas und Wasserstoff nach §§ 15a ff. EnWG** enthalten detaillierte Informationen zu künftigen Netzstrukturen und Ausbaumaßnahmen. Die erforderliche Transparenz der Netzplanung sollte erhalten bleiben, ohne sicherheitsrelevante Detailinformationen öffentlich zugänglich zu machen.

SWM-Forderung: Die gesetzlichen Vorgaben sollten daraufhin überprüft werden, inwieweit die öffentlich bereitzustellenden Informationen auf das unionsrechtlich erforderliche Maß reduziert

werden können. Geeignete Angaben sind insbesondere Korridore anstelle konkreter Trassenverläufe sowie Angaben zum Ausbaubedarf anstelle detaillierter technischer Parameter. Soweit die Vorgaben zu detailreichen Veröffentlichungen auf europäischem Recht beruhen, sollte die Bundesregierung eine entsprechende Überprüfung und Anpassung auf EU-Ebene anstoßen.

5. Veröffentlichung von Netzstrukturdaten nach § 23c EnWG begrenzen

§ 23c EnWG verpflichtet Strom- und Gasnetzbetreiber zur **Veröffentlichung umfangreicher Netzstruktur- und Betriebsdaten**. Hierzu zählen unter anderem Leitungslängen, Umspannleistungen, Entnahmestellen, versorgte und geografische Flächen, Netzanschlussdaten, Ausspeisepunkte und Jahreshöchstlasten. Darüber hinaus umfasst das geltende Veröffentlichungsregime beispielsweise viertelstündliche Last- und Netzangaben der Übertragungsnetzbetreiber (ÜNB).

Diese Angaben lassen einzeln betrachtet nicht zwingend unmittelbare Rückschlüsse auf die tatsächliche Netztopologie zu. Durch ihre Zusammenführung und Verknüpfung mit weiteren öffentlich zugänglichen Informationen können jedoch erhebliche Sicherheitsrisiken entstehen. So müssen Netzbetreiber bereits heute detaillierte Werte zu Leitungslängen nach Spannungsebene, Umspannleistung, Entnahmestellen und räumlichen Netzflächen veröffentlichen. In der Zusammenschau können solche Angaben Rückschlüsse auf Struktur, Kapazität und Auslastung der Netze sowie auf die Bedeutung einzelner Versorgungsbereiche ermöglichen. Das vom Referentenentwurf ausdrücklich anerkannte Risiko der Informationsaggregation muss daher für das gesamte Veröffentlichungsregime des § 23c EnWG berücksichtigt werden, statt lediglich einzelne Datenfelder herauszugreifen.

SWM-Forderung: § 23c EnWG sollte insgesamt unter einem ausdrücklichen KRITIS-Sicherheitsvorbehalt stehen. Daten dürfen nicht veröffentlicht werden, soweit sie allein oder in Kombination mit anderen öffentlich verfügbaren Informationen Rückschlüsse auf Lage, Struktur, Kapazität, Auslastung, Redundanzen, Engpässe oder Verwundbarkeiten kritischer Energieinfrastrukturen ermöglichen. Der Schutzvorbehalt muss sämtliche Veröffentlichungspflichten der Vorschrift erfassen und darf sich nicht auf einzelne Absätze oder Datenfelder beschränken. Soweit europarechtliche Vorgaben entgegenstehen, sollte sich die Bundesregierung auf EU-Ebene für eine entsprechende Anpassung einsetzen.

6. Sicherheitsrelevante Redispatch-, Engpass- und Systemführungsdaten schützen

Veröffentlichungen zu Redispatch-, Engpassmanagement- und Systemführungsmaßnahmen können Rückschlüsse auf wiederkehrende Netzengpässe, besonders belastete Netzbereiche, systemrelevante Anlagen und die betriebliche Reaktion der Netzbetreiber ermöglichen. Besonders kritisch sind anlagen-, ressourcen-, stations-, netzknoten- oder betriebsmittelscharfe sowie zeitlich hoch aufgelöste Angaben. Auch wenn einzelne Datensätze für sich genommen keine unmittelbare Gefährdung begründen, kann ihre Verknüpfung mit Netzstruktur-, Anlagen-, Verfügbarkeits- und Standortdaten ein detailliertes Bild neuralgischer Netzpunkte und betrieblicher Verwundbarkeiten ergeben.

SWM-Forderung: Veröffentlichungs- und Transparenzpflichten zu Redispatch-, Engpassmanagement-, Systemführungs-, Störungs- und Verfügbarkeitsdaten sind systematisch auf ihre Sicherheitsrelevanz zu überprüfen. Anlagen-, ressourcen-, stations-, netzknoten- und betriebsmittelscharfe Angaben müssen von der öffentlichen Bereitstellung ausgenommen werden, wenn sie allein oder in Verbindung mit anderen zugänglichen Informationen Rückschlüsse auf neuralgische Netzbereiche, systemrelevante Anlagen, betriebliche Engpässe oder strukturelle

Verwundbarkeiten ermöglichen. Soweit eine Veröffentlichung zur Markttransparenz erforderlich ist, sollte sie räumlich und zeitlich aggregiert, abstrahiert und mit angemessener zeitlicher Verzögerung erfolgen. Erforderliche Detailinformationen sollten ausschließlich über geschützte und zugangsbeschränkte Kommunikationswege bereitgestellt werden.

7. Schutz kritischer Anlagen im Marktstammdatenregister stärken

Öffentlich zugängliche Angaben im **Marktstammdatenregister nach § 111e EnWG**, insbesondere zu Anlagenstandorten, Betreibern, Leistungen, Netzzuordnungen und technischen Stammdaten, können in ihrer Kombination sicherheitsrelevant sein. Der Schutz kritischer Anlagen sollte nicht von einem aufwendigen Einzelnachweis der Schutzbedürftigkeit abhängen.

SWM-Forderung: Die Schutzregelung in § 15 Abs. 1 Satz 1 Nr. 1 Buchst. c MaStRV sollte so ausgestaltet werden, dass bei sicherheitsrelevanten Daten kritischer Anlagen grundsätzlich von einer besonderen Schutzbedürftigkeit ausgegangen wird. Ein zusätzlicher Nachweis durch den Betreiber sollte insoweit entfallen. Diese Daten sollten grundsätzlich von der öffentlichen Darstellung ausgenommen werden. Hilfsweise kann eine räumlich aggregierte Veröffentlichung, beispielsweise auf Gemeinde- oder Postleitzahlenebene, erfolgen, wenn auch unter Einbeziehung weiterer veröffentlichter Angaben keine sicherheitsrelevanten Rückschlüsse auf einzelne Anlagen möglich sind.

8. Nationale Transparenzplattformen auf Erforderlichkeit und Datenumfang überprüfen

Die vorgesehene Änderung von § 111g Abs. 2 Satz 9 EnWG ist positiv zu bewerten. Sicherheitsrelevante Daten sollen auf der nationalen **Transparenzplattform HEDWIG** nicht veröffentlicht werden dürfen. Der Schutz darf jedoch nicht erst bei der Veröffentlichung ansetzen: Auch die vorgelagerte Erhebung, Zusammenführung und zentrale Speicherung sensibler energiewirtschaftlicher Daten können Risiken und zudem bürokratische Aufwände verursachen.

Es bestehen Überschneidungen mit Datenbeständen von SMARD, dem Marktstammdatenregister, der ENTSO-E-Transparenzplattform sowie Veröffentlichungen der Netzbetreiber nach § 23c EnWG. Erneute Abfragen bereits gemeldeter Daten verursachen vermeidbaren Mehraufwand, insbesondere für Verteilernetzbetreiber. Zugleich kann die zentrale Zusammenführung bereits öffentlich verfügbarer Informationen neue sicherheitsrelevante Rückschlüsse auf einzelne Anlagen und Betreiber ermöglichen. Der Ausschluss von Geschäfts- und Betriebsgeheimnissen von der Veröffentlichung beseitigt zudem nicht die Risiken ihrer Erhebung und zentralen Speicherung. Aus Sicht der SWM rechtfertigt der bislang nicht erkennbare Zusatznutzen von HEDWIG gegenüber bestehenden Angeboten die zusätzlichen Sicherheitsrisiken und Meldeaufwände nicht.

Zudem sollte bei der nationalen **Informationsplattform SMARD nach § 111d EnWG** geprüft werden, welche Daten zusätzlich zu bestehenden europäischen Veröffentlichungspflichten tatsächlich erforderlich sind.

SWM-Forderung: Die SWM sprechen sich für einen vollständigen Verzicht auf die Datenerhebung im Rahmen von HEDWIG aus, um den Schutz kritischer Infrastrukturen zu stärken und Doppel- und Mehrfacherhebungen zu vermeiden. Die gesetzliche Grundlage ist entsprechend anzupassen; ein bloßes Veröffentlichungsverbot oder eine Begrenzung des Datenumfangs reicht nicht aus. Bei SMARD sollte der Datensatz auf das erforderliche Maß reduziert werden. Bereits verfügbare Daten sind vorrangig zu nutzen; zusätzliche Meldepflichten, Doppel- und Mehrfacherhebungen sowie parallele Datenbestände und redundante Veröffentlichungen sind zu vermeiden.

9. Schutz in Planungs-, Genehmigungs- und Beteiligungsverfahren stärken

Planungs- und Genehmigungsverfahren für Energie-, Wärme-, Wasser-, Abwasser-, Verkehrs- und Telekommunikationsinfrastrukturen erfordern regelmäßig detaillierte technische Unterlagen. Öffentlich ausgelegte oder über digitale Genehmigungsportale zugängliche Dokumente können genaue Anlagenstandorte, Trassenverläufe, Leitungsführungen, technische Konfigurationen, Kapazitäten, Betriebsbereiche, Zufahrten, Schutzmaßnahmen und Redundanzen erkennen lassen. Die notwendige Öffentlichkeitsbeteiligung setzt nicht voraus, dass sicherheitsrelevante technische Details ohne Zugangsbeschränkung veröffentlicht werden.

SWM-Forderung: Im Bundes-Immissionsschutzgesetz, Baugesetzbuch, Raumordnungsgesetz, Umweltverträglichkeitsprüfungsgesetz und in weiteren einschlägigen Planungs- und Genehmigungsvorschriften sollte ein einheitlicher Schutzvorbehalt für sicherheitsrelevante Infrastrukturinformationen verankert werden. Vor jeder öffentlichen Auslegung oder digitalen Bereitstellung ist zu prüfen, ob Unterlagen die Identifikation kritischer Anlagen, neuralgischer Infrastrukturpunkte oder sicherheitsrelevanter Betriebs- und Schutzkonzepte ermöglichen. Entsprechende Inhalte müssen geschwärzt, abstrahiert oder aus der öffentlichen Fassung entfernt werden können. Für die Öffentlichkeitsbeteiligung ist eine sicherheitsbereinigte Fassung bereitzustellen; erforderliche Detailunterlagen dürfen nur einem legitimierten und zur Vertraulichkeit verpflichteten Personenkreis zugänglich sein.

10. Sicherheitsrelevante Infrastrukturinformationen in Vergabeverfahren schützen

Auch bei der Beschaffung muss der Schutz kritischer Infrastrukturen gewährleistet sein. Die für einen wirksamen Wettbewerb erforderliche Transparenz darf nicht dazu führen, dass sensible Infrastrukturinformationen uneingeschränkt zugänglich werden. Notwendig ist eine klare Unterscheidung zwischen öffentlich bereitzustellenden Angaben und schutzbedürftigen Detailunterlagen.

SWM-Forderung: Die Regelungen im Gesetz gegen Wettbewerbsbeschränkungen (GWB), in der Vergabeverordnung und in der Sektorenverordnung sollten gezielt auf den Schutz sicherheitsrelevanter Infrastrukturinformationen überprüft und entsprechend weiterentwickelt werden. Dabei ist ein abgestufter Informationszugang vorzusehen: Öffentliche Bekanntmachungen müssen ausreichend über den Auftragsgegenstand und die Voraussetzungen für die Teilnahme am Wettbewerb informieren, ohne sensible Details offenzulegen. Schutzbedürftige Unterlagen dürfen erst nach Prüfung der Zugangsberechtigung und unter angemessenen Vertraulichkeitsauflagen bereitgestellt werden. Die hierfür geltenden Anforderungen müssen auf objektiven, diskriminierungsfreien Kriterien beruhen und für Auftraggeber sowie teilnehmende Unternehmen mit vertretbarem Aufwand umsetzbar sein. Ergänzend sollte die Sicherheitsausnahme nach § 107 Abs. 2 GWB im unionsrechtlich zulässigen Rahmen auf Aufträge im Zusammenhang mit der Planung, dem Bau, dem Betrieb und insbesondere dem Schutz von Anlagen im Bereich kritischer Infrastrukturen erweitert werden.

11. Sektorübergreifenden Schutz kommunaler Infrastrukturen sicherstellen

Kritische Infrastrukturen sind eng miteinander verbunden. Strom-, Gas- und Wärmeversorgung, Wasserver- und Abwasserentsorgung, Telekommunikation sowie öffentlicher Verkehr sind aufeinander angewiesen. Informationen über eine Infrastruktur können deshalb Rückschlüsse auf andere Versorgungsbereiche ermöglichen. Ein rein sektorspezifischer Schutz einzelner Veröffentlichungen greift zu kurz.

SWM-Forderung: Die Überprüfung gesetzlicher Transparenz-, Veröffentlichungs- und Informationspflichten muss alle relevanten Sektoren der öffentlichen Daseinsvorsorge umfassen. Neben Elektrizität, Gas und Wasserstoff sind insbesondere Wärme, Wasser und Abwasser, Telekommunikation und Informationstechnik sowie öffentlicher Personennahverkehr einzubeziehen.

Bei kritischen Anlagen und Einrichtungen des **öffentlichen Personennahverkehrs** muss sichergestellt werden, dass sicherheitsrelevante Informationen, etwa zu Standorten, Trassen, Bauwerksstrukturen, technischen Anlagen, Kapazitäten oder Schutzvorkehrungen, nicht aufgrund gesetzlicher Transparenz-, Informations- oder Veröffentlichungspflichten offengelegt werden müssen.

Für die **Trinkwasserversorgung** sind ebenfalls entsprechende Schutzregelungen vorzusehen. Sicherheitsrelevante Angaben über Anlagen und Netze müssen insbesondere in wasserrechtlichen Verfahren, Planungsunterlagen und Geodatenangeboten wirksam geschützt werden. Informationen, die auf einem dieser Wege aus Sicherheitsgründen zurückgehalten werden, dürfen nicht über andere Informationsansprüche oder Veröffentlichungspflichten offengelegt werden. Erforderliche Informations- und Beteiligungsrechte bleiben dabei gewahrt.

Für die **Telekommunikation** sind die Informations- und Datenbereitstellungspflichten im Telekommunikationsgesetz, insbesondere im Zusammenhang mit dem Gigabit-Grundbuch, entsprechend anzupassen. Sicherheitsrelevante Infrastruktur- und Baustellendaten müssen wirksam geschützt werden. Dabei sind auch Telekommunikationsinfrastrukturen einzubeziehen, deren Ausfall andere kritische Infrastrukturen beeinträchtigen würde. Anstelle einer zentralen Speicherung detaillierter Infrastrukturdaten sollte ein dezentraler Infrastrukturatlas vorgesehen werden, bei dem die Daten bei den Infrastrukturinhabern verbleiben und nur zweckgebunden für berechtigte Stellen zugänglich sind. Die Einstufung als kritische Infrastruktur sollte für Ausnahmen von Datenlieferungspflichten ausreichen, ohne zusätzliche Nachweise einer besonderen Schutzbedürftigkeit zu verlangen.

Für alle kritischen Sektoren sollten einheitliche Mindestgrundsätze gelten: Vorrang der Datenminimierung, Veröffentlichung nur im erforderlichen Umfang, Aggregation und Anonymisierung sicherheitsrelevanter Angaben, Schutz vor sektorübergreifender Datenverknüpfung sowie verbindliche Anforderungen an Zugriff, Speicherung, Weitergabe und Löschung.

12. Europäischen Rechtsrahmen einbeziehen

Ein Teil der energiewirtschaftlichen Transparenzpflichten beruht unmittelbar auf europäischem Recht. Dies gilt insbesondere für die europäische Strom-Transparenzplattform nach der Verordnung (EU) Nr. 543/2013 sowie für Vorgaben zu Netzplanung und Netzentwicklung, die auf der Elektrizitätsbinnenmarkt-Richtlinie (EU) 2019/944 (EBMRL) und der Gas- und Wasserstoffrichtlinie (EU) 2024/1788 beruhen. Nationale Anpassungen allein können die bestehenden Schutzlücken daher nicht vollständig schließen.

SWM-Forderung: Die Bundesregierung sollte sich auf europäischer Ebene für eine systematische Überprüfung bestehender Transparenz- und Veröffentlichungspflichten einsetzen. Angemessene KRITIS-Ausnahmen sollten für alle betroffenen Netzbetreiber und entlang der gesamten energiewirtschaftlichen Wertschöpfungskette vorgesehen werden. Insbesondere ist für Verteilernetzbetreiber in der Verordnung (EU) Nr. 543/2013 eine eigenständige Ausnahmeregelung analog zu bestehenden Schutzmöglichkeiten für Übertragungsnetzbetreiber erforderlich.

III. Zusammenfassung

Die SWM unterstützen das Ziel des Referentenentwurfs, dem Schutz kritischer Infrastrukturen bei Transparenz-, Informations- und Veröffentlichungspflichten stärker Rechnung zu tragen. Die vorgeschlagenen Änderungen an den §§ 12f und 111g EnWG sowie am Informationsfreiheitsgesetz sind hierfür wichtige erste Schritte.

Der Handlungsbedarf geht jedoch darüber hinaus. Anstelle einer lediglich punktuellen Korrektur einzelner Veröffentlichungspflichten ist im EnWG und in weiteren infrastrukturelevanten Fachgesetzen ein einheitlicher KRITIS-Schutzvorbehalt zu verankern.

Für den Energiesektor sollten insbesondere die Vorgaben zu Netzstrukturdaten, Netzausbau- und Netzentwicklungsplänen, dem Marktstammdatenregister sowie nationalen und europäischen Transparenzplattformen in den angekündigten weiteren Prüfprozess einbezogen werden. Darüber hinaus sind auch in weiteren KRITIS-Sektoren, etwa im öffentlichen Personennahverkehr und in der Wasserversorgung, die einschlägigen Transparenz-, Veröffentlichungs- und Informationspflichten zu überprüfen und zum Schutz sicherheitsrelevanter Infrastrukturinformationen anzupassen.

Dabei sollte ein einheitlicher Grundsatz gelten: Transparenz bleibt ein wichtiges regulatorisches Ziel. Sie darf jedoch nicht dazu führen, dass Informationen öffentlich zugänglich werden, die einzeln oder in Kombination die Identifikation kritischer Anlagen, neuralgischer Netzpunkte oder struktureller Verwundbarkeiten erleichtern.