Energie. Wasser. Leben.

Berlin, 17. November 2026

BDEW Bundesverband der Energie- und Wasserwirtschaft e.V.

Reinhardtstraße 32
10117 Berlin

www.bdew.de

Stellungnahme

Gesetz zur Anpassung von Transparenz-, Veröffentlichungs- und Informationspflichten zum angemessenen Schutz kritischer Infrastrukturen

Transparenz-Register-ID des BDEW: 20457441380-38

Der Bundesverband der Energie- und Wasserwirtschaft (BDEW), Berlin, und seine Landesorganisationen vertreten mehr als 2.000 Unternehmen. Das Spektrum der Mitglieder reicht von lokalen und kommunalen über regionale bis hin zu überregionalen Unternehmen. Sie repräsentieren rund 90 Prozent des Strom- und gut 60 Prozent des Nah- und Fernwärmeabsatzes, über 90 Prozent des Erdgasabsatzes, über 95 Prozent der Energienetze sowie 80 Prozent der Trinkwasser-Förderung und rund ein Drittel der Abwasser-Entsorgung in Deutschland.

Der BDEW ist im Lobbyregister für die Interessenvertretung gegenüber dem Deutschen Bundestag und der Bundesregierung sowie im europäischen Transparenzregister für die Interessenvertretung gegenüber den EU-Institutionen eingetragen. Bei der Interessenvertretung legt er neben dem anerkannten Verhaltenskodex nach § 5 Absatz 3 Satz 1 LobbyRG, dem Verhaltenskodex nach dem Register der Interessenvertreter (europa.eu) auch zusätzlich die BDEW-interne Compliance Richtlinie im Sinne einer professionellen und transparenten Tätigkeit zugrunde. Registereintrag national: R000888. Registereintrag europäisch: 20457441380-38

Vorbemerkung zu den Anhörungsfristen

Der Koalitionsvertrag von CDU, CSU und SPD sieht für die Beteiligung von Betroffenen und Vollzugsexperten in der Frühphase von Gesetzgebungsverfahren angemessene Fristen von in der Regel vier Wochen vor (Zeilen 1865–1870). Für die Verbändeanhörung zum vorliegenden Referentenentwurf ist hingegen lediglich der Zeitraum vom 5. bis zum 17. November 2026 vorgesehen. Dies entspricht neun Arbeitstagen bei einer Arbeitswoche von Montag bis Freitag. Eine solche Frist erschwert die Rückkopplung in den Verbänden mit ihren Mitgliedsunternehmen erheblich und lässt eine umfassende Prüfung der Praxisfolgen und Rechtsfragen kaum zu. Die Beteiligung im nachgelagerten parlamentarischen Verfahren ersetzt eine fundierte fachliche Befassung in der Frühphase nicht. Anhörungsverfahren müssen ihren Beitrag zur Vorbereitung praxistauglicher und vollständiger Regelungen leisten können. Der BDEW fordert deshalb, die im Koalitionsvertrag vorgesehenen Beteiligungsfristen einzuhalten.

Einleitung und Positionen im Überblick

Der Bundesverband der Energie- und Wasserwirtschaft e. V. (BDEW) begrüßt das Ziel des Referentenentwurfs des Bundesministeriums des Innern eines Gesetzes zur Anpassung von Transparenz-, Veröffentlichungs- und Informationspflichten zum angemessenen Schutz kritischer Infrastrukturen (Stand: 30.09.2026), die geltenden Transparenz-, Veröffentlichungs- und Informationspflichten an die veränderte Sicherheitslage anzupassen. Der Schutz kritischer Infrastrukturen muss auch den Umgang mit Informationen über Anlagen und Netze umfassen. Öffentlich verfügbare Daten können die Vorbereitung von Sabotage und Angriffen erleichtern. Dies gilt insbesondere, wenn digitale Kartendienste und künstliche Intelligenz Informationen aus unterschiedlichen Quellen zusammenführen und auswerten.

Die vorgesehenen Änderungen des Energiewirtschaftsgesetzes (EnWG) und des Informationsfreiheitsgesetzes (IFG) sind wichtige erste Schritte. Für einen durchgängigen Schutz müssen jedoch weitere Informationswege einbezogen und die Regelungen rechtssicher im Bundes- und Landesrecht ausgestaltet werden. Dies betrifft neben der Energieversorgung ausdrücklich die Trinkwasserversorgung und die Abwasserentsorgung. Der Entwurf enthält für diese Bereiche keine spezifischen Anpassungen ihrer Veröffentlichungs- und Informationspflichten. Auch Auslegungspflichten im Rahmen von Umweltverträglichkeitsprüfungen und die Öffentlichkeitsbeteiligung in Planfeststellungsverfahren sind einzubeziehen. Bereits bestehende Schutzvorschriften sind konsequent anzuwenden und verbleibende Lücken gezielt zu schließen.

Hierzu sind auch auf Landesebene konsequent die erforderlichen Maßnahmen und Gesetzesanpassungen vorzunehmen. Auf Landesebene können beispielsweise zusätzlich presserechtliche Auskunftsansprüche gegenüber Stadtwerken bestehen, die im Sinne einer einheitlichen Rechtsordnung ebenso um Sicherheitsaspekte ergänzt werden sollten.

Ein ganzheitlicher Schutzansatz muss die gesamte Verarbeitung und öffentliche Verfügbarkeit sicherheitsrelevanter Informationen erfassen. Behörden und Plattformen der öffentlichen Hand, die Daten der Energie- und Wasserwirtschaft erheben, speichern oder bereitstellen, müssen ein dem Schutzbedarf entsprechendes IT-Sicherheitsniveau gewährleisten, das mit den Anforderungen an die betroffenen Betreiber vergleichbar ist.

Die Gesamtrisikobetrachtung muss darüber hinaus Informationen einbeziehen, die unabhängig von gesetzlichen Transparenz- und Veröffentlichungspflichten über öffentlich zugängliche Infrastrukturportale, digitale Karten- und Geodatendienste sowie Luftbild- und Straßenansichtsdienste verfügbar sind. Der BDEW fordert hierfür klare gesetzliche Befugnisse, mit denen zuständige Behörden öffentliche und private Anbieter bei sicherheitsrelevanten Risiken zu einer Einschränkung, Abstraktion oder Entfernung entsprechender Veröffentlichungen verpflichten können. Anstelle oder neben einem behördlichen Anspruch sollte der KRITIS-Betreiber selbst die Löschung unmittelbar gegenüber dem Kartenanbieter geltend machen können. Der Anspruch sollte unmittelbar und gebunden sein. Die Einstufung als kritische Anlage sowie das überragende öffentliche Interesse am Betrieb der Energie- und/oder Wasserinfrastruktur sollten dazu führen, dass eine erneute Einzelfallprüfung der Gefahrenlage oder eine Abwägung mit entgegenstehenden Interessen des Betreibers oder sonstiger Dritter entfallen kann. Das Verfahren sollte sich auf die eindeutige Bezeichnung der Anlage, des räumlichen Bereichs und der verlangten Maßnahme beschränken. Eine behördliche Bestätigung sollte keine Anspruchsvoraussetzung sein.

Auch Unternehmens- und Standortadressen sowie personenbezogene Angaben, etwa zu Beschäftigten und Ansprechpersonen, können Spionage und gezielte Phishing-Angriffe auf einzelne Personen (Spear-Phishing) erleichtern. Die einschlägigen Offenlegungs- und Registervorschriften sind deshalb ebenfalls um risikogerechte Schutzregelungen und abgestufte Zugangsrechte zu ergänzen. Erforderlich ist eine verhältnismäßige Ausgestaltung, die berechtigte Transparenzinteressen wahrt und zugleich sicherheitskritische Rückschlüsse wirksam begrenzt. Die Transparenz über politische Interessenvertretung und Zuwendungen bleibt davon unberührt.

Die Stellungnahme bezieht sich auf den zur Verbändebeteiligung übersandten Referentenentwurf mit Bearbeitungsstand vom 30. September 2026. Im Mittelpunkt stehen folgende Positionen:

- **Sicherheitsrelevante Daten wirksam schützen.** Die Änderungen an §§ 12f und 111g EnWG sind zu unterstützen. Einheitliche Kriterien müssen auch die Verknüpfung mehrerer Datensätze und die räumliche sowie zeitliche Auflösung berücksichtigen.

- **Den IFG-Ausschluss rechtssicher fassen.** Änderungsbefehl, Schutzbereich und Begründung sind aufeinander abzustimmen.
- **Schutzlücken zwischen Informationswegen schließen.** Genehmigungsrecht, Umweltinformationsrecht, Geodatenrecht und landesrechtliche Transparenzvorgaben müssen ein vergleichbares Schutzniveau gewährleisten.
- **Genehmigungsrecht in dieses Gesetz aufnehmen.** Das Bundes-Immissionsschutzgesetz ist in das Artikelgesetz aufzunehmen. Sicherheitsrelevante Antragsunterlagen sind kraft Gesetzes von der Internetveröffentlichung auszunehmen. Der Schutz muss auch für geplante und in Errichtung befindliche Anlagen gelten.
- **Weitere BDEW-Prioritäten verbindlich umsetzen.** Für den Infrastrukturatlas, Kapazitätskarten, Netzausbaupläne (§ 14d EnWG) der VNB sowie die Netzentwicklungspläne der ÜNB, Vergabeverfahren und die Digitale Plattform Unbemannte Luftfahrt (dipul) sind konkrete Anpassungen und ein ressortübergreifender Zeitplan erforderlich.
- **Bestehende Veröffentlichungen einbeziehen.** Angesichts der veränderten geopolitischen und sicherheitspolitischen Rahmenbedingungen muss der Schutz kritischer und sicherheitsrelevanter Informationen Vorrang haben. Informationen, die in der Vergangenheit aus Gründen der Transparenz veröffentlicht wurden, können heute ein erhebliches Sicherheitsrisiko darstellen. Transparenz darf daher nicht dazu führen, dass sensible Informationen zu früh, zu umfassend oder gegenüber einem nicht hinreichend bestimmten Teilnehmerkreis offengelegt werden. Erforderlich sind klare und rechtssichere Vorgaben, die eine Veröffentlichung auf das notwendige Maß begrenzen und sicherstellen, dass sicherheitsrelevante Informationen nur dann und nur gegenüber denjenigen Wirtschaftsteilnehmern zugänglich gemacht werden, bei denen dies für das konkrete Verfahren erforderlich und aus Sicherheitsgründen vertretbar ist. Zudem sind Zuständigkeiten und Verfahren für die Prüfung, Beschränkung oder Entfernung sicherheitskritischer Informationen festzulegen. Der Zugang zu Detaildaten muss sich am tatsächlichen Informationsbedarf orientieren.
- **Einen einheitlichen Schutzvorbehalt verankern.** Sicherheitsrelevante Informationspflichten sind über einzelne Vorschriften hinaus konsistent zu begrenzen. Aktuelle Betriebs- und Projektdaten bedürfen eines besonders strengen, aufgabenbezogenen Zugangs. Die Anpassungen des Telekommunikationsrechts und des Gigabit-Grundbuchs sind ausdrücklich einzubeziehen.

1. Sicherheitsrelevante Netzdaten konsequent schützen

Ergänzend zu den vorgesehenen Einzeländerungen fordert der BDEW einen **übergreifenden Schutzvorbehalt für die gesetzlichen Informations-, Transparenz-, Datenbereitstellungs- und**

Veröffentlichungspflichten des EnWG und der auf seiner Grundlage erlassenen Rechtsverordnungen.

Sicherheitsrelevante Informationen dürfen nicht veröffentlicht oder allgemein zugänglich gemacht werden, wenn sie allein oder zusammen mit anderen zugänglichen Informationen geeignet sind, die Sicherheit oder Zuverlässigkeit von Energieversorgungsnetzen oder Energieanlagen zu gefährden. Dies umfasst insbesondere sicherheitskritische Rückschlüsse auf Anlagen, neuralgische Netzpunkte, Redundanzen, Engpasssituationen oder strukturelle Verwundbarkeiten. Erfasst sein müssen Elektrizitäts-, Gas-, Wasserstoff- und Wärmeinfrastrukturen einschließlich Erzeugungsanlagen, Energiespeicheranlagen, Elektrolyseure und die jeweiligen Netzanschlusspunkte.

Der Schutzansatz muss außerdem die für den Betrieb der Infrastrukturen erforderlichen Informations- und Kommunikationstechnologien erfassen und erforderlichenfalls in den jeweils einschlägigen Fachgesetzen ergänzt werden. Aggregierte, abstrahierte, kategorisierte oder anonymisierte Angaben müssen Vorrang vor der Offenlegung detaillierter Informationen haben, sofern damit sicherheitskritische Rückschlüsse tatsächlich ausgeschlossen werden. Notwendige aufgabenbezogene Datenzugänge sind gesondert abzusichern.

1.1. Aufgabenbezogenen Datenzugang praxistauglich ausgestalten (zu Artikel 1 Nummer 1 – § 12f Absatz 2 EnWG-E)

Der BDEW unterstützt, die Herausgabe detaillierter Netzdaten an nachgewiesene Fachkunde und die Erforderlichkeit für die jeweilige Aufgabe zu knüpfen. Der ausdrückliche Schutz sicherheitsrelevanter Daten neben Betriebs- und Geschäftsgeheimnissen ist sachgerecht: Informationen können für die Versorgungssicherheit schutzbedürftig sein, ohne zugleich ein Unternehmensgeheimnis darzustellen. Netzknotenpunktscharfe Einspeisedaten lassen zudem Rückschlüsse auf einzelne Erzeugungs- und Speicheranlagen zu und sind auch aus diesem Grund schutzbedürftig.

Die Anforderungen an Fachkunde, Aufgabenerforderlichkeit und Vertraulichkeit müssen einheitlich und nachvollziehbar angewendet werden. Positiv ist, dass § 12f Abs. 2 Satz 3 EnWG-E „sicherheitsrelevante Daten“ von der Herausgabe nach Satz 1 explizit ausnimmt.

Für die Sicherheitsbewertung nach Satz 3 („sicherheitsrelevant“) sind Kriterien gemeinsam mit den zuständigen Behörden und den betroffenen Betreibern zu entwickeln. Hier wäre ein Leitfaden denkbar, der sich auch mit Regelbeispielen befasst. Maßgeblich sind insbesondere mögliche Rückschlüsse auf Netzstrukturen, betriebliche Abhängigkeiten und Schutzvorkehrungen. Auch die Kombination mit anderen öffentlich verfügbaren Daten ist einzubeziehen. Eine Sicherheitsrelevanz darf nicht erst bei Nachweis einer konkreten Angriffsvorbereitung angenommen werden.

Bei der Sicherheitsbewertung ist ausdrücklich zwischen statischen Bestandsinformationen und aktuellen beziehungsweise in Echtzeit verfügbaren Betriebs- und Projektdaten zu unterscheiden. Aktuelle Netzauslastungen, verfügbare Kapazitäten, Engpassinformationen sowie aktuelle Angaben aus Genehmigungsverfahren, Entwicklungsplänen und Projekten können unmittelbar nutzbare Rückschlüsse auf die Betriebslage ermöglichen. Für diese Informationen ist ein besonders strenges Need-to-know-Prinzip vorzusehen: Zugang nur bei nachgewiesenem Aufgabenbedarf und beschränkt auf den erforderlichen Datenumfang, Zweck, Personenkreis und Zeitraum. Ihre Überprüfung und Zugriffsbeschränkung sind vorrangig anzugehen, weil hier kurzfristig ein Sicherheitsgewinn erreichbar ist. Auch statische und bereits bekannte Daten bleiben schutzbedürftig, insbesondere bei systematischer Zusammenführung.

Für georeferenzierte Daten sind die Kriterien durch nachvollziehbare Anwendungsbeispiele zu konkretisieren. So können räumliche Leitungsverläufe in Verbindung mit Angaben zu Anlagenstandorten, technischer Auslegung oder aktuellen Kapazitäten zusätzliche Rückschlüsse auf betriebliche Abhängigkeiten und besonders relevante Netzbereiche ermöglichen. Entscheidend sind der zusätzliche Erkenntnisgewinn durch die Verknüpfung und die daraus entstehenden Sicherheitsrisiken; nicht jede Kombination von GIS-Daten ist automatisch sicherheitskritisch.

Die Pflicht zur ersatzweisen Bereitstellung typisierter Datensätze muss unter einem ausdrücklichen Sicherheitsvorbehalt stehen. Typisierung darf keine Rekonstruktion geschützter Informationen ermöglichen. Der BDEW fordert daher eine Klarstellung, dass Ersatzdaten nur in einer Form herausgegeben werden dürfen, die auch unter Berücksichtigung ihrer Verknüpfbarkeit keine sicherheitskritischen Rückschlüsse zulässt. Dies gilt ebenso für standardisierte, elektronisch verarbeitbare Formate.

1.2. Veröffentlichungsverbot auf der Transparenzplattform absichern (zu Artikel 1 Nummer 2 – § 111g Absatz 2 Satz 9 EnWG)

Der BDEW begrüßt das vorgesehene Veröffentlichungsverbot für die von der Regelung erfassten Daten („die geeignet sind, die Sicherheit oder Zuverlässigkeit der Elektrizitäts-, Gas- oder Wasserstoffversorgungssysteme oder die Sicherheit und Ordnung zu gefährden, oder die europäischen kritischen Anlagen betreffen“). Die bisherige Möglichkeit einer Veröffentlichung im Einvernehmen mit den Übertragungsnetzbetreibern entfällt. Ebenso sachgerecht ist die ausdrückliche Einbeziehung von Gas- und Wasserstoffversorgungssystemen. In der Gesetzesbegründung sollte klargestellt werden, dass der Begriff der Versorgungssysteme weit zu verstehen ist und alle relevanten Anlagen umfasst, also über die Leitungen hinausgeht und dabei etwa auch die angeschlossenen Erzeugungs- und Energiespeicheranlagen umfasst.

Vor jeder Veröffentlichung sind Datentiefe und Kombinationsrisiken zu prüfen, damit das Verbot nach § 111g Abs. 2 Satz 9 EnWG-E wirksam wird. Betroffene Betreiber sollten ihre

Sicherheitsbewertung dabei frühzeitig einbringen können. Der Schutz ist auch bei Schnittstellen, Downloads und späteren Aktualisierungen zu gewährleisten.

Wir empfehlen deshalb, § 111g Absatz 2 Satz 9 EnWG-E 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 europäischen kritischen Anlagen betreffen, nicht veröffentlichen **und stellt über die sicherheitsgefährdende Eigenschaft von Daten vor Veröffentlichung das Einvernehmen mit dem jeweiligen Betreiber des Elektrizitäts-, Gas- oder Wasserstoffversorgungssystems her**; Absatz 1 Satz 1 bleibt hiervon unberührt. […]“

Die Datenerhebungsbefugnis nach § 111g Absatz 1 Satz 1 EnWG bleibt im vorliegenden Referentenentwurf unberührt. Veröffentlichungsschutz und Datenlieferpflichten sind zwar zu unterscheiden. Aber auch Erhebung, Speicherung, behördlicher Zugriff und Weiterverarbeitung müssen auf den erforderlichen Umfang begrenzt und sicher ausgestaltet sein.

Die Änderung des § 111g EnWG schafft keine entsprechende Schutzregelung für andere Register und Plattformen. Deren Vorgaben müssen gesondert überprüft und angepasst werden.

2. Den Informationszugang rechtssicher begrenzen (zu Artikel 2 – § 3 IFG)

Ein eigenständiger Schutz sicherheitsrelevanter Infrastrukturinformationen im IFG entspricht einem zentralen Anliegen des BDEW. Zu begrüßen ist, dass auch besonders schutzbedürftige Infrastrukturen außerhalb einer formalen KRITIS-Einstufung erfasst werden sollen. Für die sichere Versorgung können auch Anlagen und Netze unterhalb gesetzlicher Schwellenwerte oder im Zusammenwirken mit anderen Infrastrukturen wesentlich sein.

Da das IFG nur gegenüber Behörden des Bundes gilt, müssen die Bundesländer zügig ihre Landes-IFG ebenfalls anpassen.

Auch der materielle Maßstab muss eindeutig sein. Während der vorgeschlagene Wortlaut allgemein an Informationen hinsichtlich bestimmter Infrastrukturen anknüpft, beschreibt die Begründung mögliche nachteilige Auswirkungen ihres Bekanntwerdens. Der BDEW fordert einen eigenständigen Ausschlussgrund, der diesen Widerspruch beseitigt. Er muss auch Informationen erfassen, die erst zusammen mit anderen Daten sicherheitskritische Rückschlüsse ermöglichen.

Grundsätzlich ist zu begrüßen, dass für KRITIS-Anlagen kein Anspruch auf Informationszugang besteht. Für die Anwendung der Regelung auf andere „besonders schutzbedürftige Anlagen“ sollten typische schutzbedürftige Informationskategorien und belastbare Kriterien aus Gründen der Rechtssicherheit im Normtext konkretisiert werden. Dazu gehören insbesondere

sicherheitsrelevante Angaben zu Standorten, Leitungen und Trassen, technischer Auslegung, Kapazitäten, Verwundbarkeiten und Schutzvorkehrungen. Die Regelbeispiele müssen bestehende, in Errichtung befindliche und geplante Anlagen erfassen. Ein Tatbestand mit erkennbarer Schadensschwelle und Regelbeispielen ist deshalb rechtssicherer als ein pauschaler Ausschluss. Ein Formulierungsvorschlag ist als Anlage 2 beigefügt. Nachvollziehbare, auf die betroffene Informationskategorie bezogene Sicherheitsbewertungen müssen ausreichen. Ein bereits konkretisierter Angriff darf keine Voraussetzung sein. Ebenso wenig sollten Unternehmen sensible Einzelheiten offenlegen müssen, um gerade deren Schutz zu begründen.

Sicherheitsbezogene Begründungen und Nachweise müssen selbst vertraulich behandelt werden können. Soweit sich der Informationszweck durch geschwärzte oder hinreichend abstrahierte Unterlagen erreichen lässt, ist diese Form vorzusehen. Das ermöglicht eine sachgerechte Wahrnehmung von Informations- und Beteiligungsrechten bei wirksamem Schutz sicherheitsrelevanter Details. Der Ausschlussgrund zielt auf sicherheitsrelevante Anlagen- und Netzdetails. Informationen über Kosten, Förderentscheidungen oder Emissionen sind nicht sein Gegenstand; dies sollte in der Begründung klargestellt werden.

Ergänzend benötigen Betreiber ein gesetzlich abgesichertes Recht, die Herausgabe sicherheitsrelevanter Informationen zu verweigern, wenn deren Offenlegung die geschützten Infrastrukturen gefährden kann. Dieses Recht muss mit den jeweiligen Informationspflichten abgestimmt werden und darf nicht durch parallele Zugangswege unterlaufen werden. Gesetzlich erforderliche aufgabenbezogene Übermittlungen an zuständige Stellen sind gesondert und unter geeigneten Schutzvorkehrungen zu regeln.

3. Vertraulichkeit auch in Gerichtsverfahren gewährleisten (zu Artikeln 4 und 5 – § 172 Nummer 1 GVG und § 52 ArbGG)

Der BDEW begrüßt die ausdrückliche Möglichkeit, die Öffentlichkeit bei einer zu befürchtenden Gefährdung kritischer Infrastrukturen auszuschließen. Dies kann insbesondere bei der Erörterung sensibler Anlageninformationen, betrieblicher Zugangsrechte oder Schutzmaßnahmen erforderlich sein.

Der Ausschluss der Verhandlungsöffentlichkeit allein gewährleistet jedoch noch keinen umfassenden Schutz sämtlicher Verfahrensunterlagen. Ergänzend ist zu prüfen, wie Akteneinsicht, elektronische Bereitstellung und die Veröffentlichung gerichtlicher Entscheidungen sicherheitsgerecht ausgestaltet werden können. Erforderlich ist ein durchgängiger Schutz unter Wahrung rechtlichen Gehörs und effektiven Rechtsschutzes.

4. Genehmigungsrecht und Informationsrechte aufeinander abstimmen

Der Entwurf baut auf dem erweiterten Geheimnisschutz des § 30 des Verwaltungsverfahrensgesetzes (VwVfG) auf. Dieser Ansatz muss in den Fachverfahren für Energie- und Wasserinfrastrukturen konsequent umgesetzt werden. Der BDEW fordert klare und verfahrensübergreifend abgestimmte Möglichkeiten, sensible Unterlagen zu schwärzen, zu abstrahieren oder nur einem berechtigten Personenkreis zugänglich zu machen. Der Schutz muss von der Antragstellung über Auslegung und Anhörung bis zur Veröffentlichung der Entscheidung reichen.

Bereits bestehende Schutzregelungen sind dabei zu berücksichtigen und konsequent anzuwenden. Für Planfeststellungsverfahren schreibt § 72a Absatz 1 VwVfG bereits die Beachtung der Anforderungen an den Geheim- und Sabotageschutz vor. Auch § 10 Absatz 2 BImSchG enthält Vorgaben zum Schutz von Unterlagen, deren Veröffentlichung nachteilige Auswirkungen auf kritische Infrastrukturen oder weitere geschützte Belange hätte. In der Praxis verlangt diese Regelung jedoch, dass der Antragsteller die Schutzbedürftigkeit für einzelne Unterlagen geltend macht und begründet. Das führt zu erheblichem Aufwand, uneinheitlichem Vollzug und Unsicherheit darüber, ob die Auslegung ordnungsgemäß war. Der weitere Anpassungsbedarf ist deshalb gezielt an verbleibenden Schutzlücken und Vollzugsproblemen auszurichten.

Dabei sind handhabbare Regelungen von besonderer Bedeutung, da gerade im Genehmigungsrecht an die Veröffentlichung von Unterlagen weitere rechtliche Konsequenzen geknüpft sind. Die hiermit verbundenen Genehmigungsrisiken müssen so weit wie möglich minimiert werden. Die Ausführungen zu typischen schutzbedürftigen Informationskategorien und belastbaren Kriterien im Abschnitt zu den IFG-Regelungen gelten insoweit entsprechend.

Die mit dem Gesetz zur Umsetzung der Richtlinie 2010/75/EU über Industrieemissionen eingefügten Regelungen zum Geheimnisschutz im Genehmigungsverfahren sind insofern nicht ausreichend. Der BDEW fordert deshalb, das Bundes-Immissionsschutzgesetz und die 9. BImSchV in das vorliegende Artikelgesetz aufzunehmen. Erforderlich ist eine gesetzliche Regelvermutung: Unterlagen mit Angaben über sicherheitsrelevante Eigenschaften, insbesondere zu Lage und Anordnung von Anlagenteilen, technischer Auslegung, Medienversorgung, Verwundbarkeiten und Schutzvorkehrungen, sind von der Auslegung und der Veröffentlichung im Internet ausgenommen. An ihre Stelle tritt eine Inhaltsdarstellung nach § 27b Absatz 4 VwVfG. Personen, die eine mögliche Betroffenheit in eigenen Belangen darlegen, und anerkannte Vereinigungen erhalten Einsicht in einem kontrollierten Verfahren. Angaben über Emissionen in die Umwelt bleiben öffentlich. Zugleich ist klarzustellen, dass die gesetzlich vorgesehene Nichtveröffentlichung keinen Verfahrensfehler begründet. Die Regelung ist zeitkritisch, weil für die im November 2026 bezuschlagten wasserstofffähigen Gaskraftwerke die Genehmigungsverfahren anlaufen oder bereits laufen. Ein Formulierungsvorschlag ist als Anlage 2 beigefügt.

Der Schutz muss ausdrücklich auch für geplante und in Errichtung befindliche Anlagen gelten. In der Projektphase liegen den Behörden die detailliertesten Unterlagen vor, während die Anlage noch nicht als kritische Anlage bestimmt ist. Der BDEW regt eine Klarstellung in § 30 VwVfG an, dass der Schutz mit der Einleitung des Zulassungsverfahrens beginnt.

Zunächst sind insbesondere § 71 EnWG und § 30a Netzausbaubeschleunigungsgesetz Übertragungsnetz sowie das Gesetz über die Umweltverträglichkeitsprüfung zu überprüfen und zu ergänzen. Gleiches gilt für das Bundesberggesetz, die Störfall-Verordnung und das Windenergie-auf-See-Gesetz, die Kavernenspeicher, Wasserstoffanlagen und Offshore-Windparks betreffen. Die im Entwurf angesprochenen weiteren Arbeiten zum Bau-, Raumordnungs- und Immissionsschutzrecht müssen mit dem vorliegenden Gesetz abgestimmt werden. Für das Immissionsschutzrecht genügt eine Abstimmung nicht; hier ist die Aufnahme in dieses Gesetz erforderlich. Ein Verweis auf parallele Verfahren genügt nur, wenn dadurch ein lückenloser und zeitnah wirksamer Schutz tatsächlich erreicht wird.

Der Anwendungsbereich der vorgesehenen Schutzregelungen sollte zudem ausdrücklich auch Kohlendioxidleitungen und Kohlendioxidleitungsnetze nach dem Kohlendioxid-Speicherung-und-Transport-Gesetz (KSpTG) erfassen. Das BMWE stellt in der Begründung zum Referentenentwurf der Kohlendioxidleitungsverordnung selbst fest, dass „Leitungen nach dem EnWG und dem KSpTG ein vergleichbares Gefahrpotenzial besitzen“. Vor diesem Hintergrund ist es sachgerecht, sicherheitsrelevante Informationen zu diesen Infrastrukturen, insbesondere zu Lage, Verlauf und technischer Ausgestaltung, einem vergleichbaren Schutzniveau zu unterstellen. Eine unterschiedliche Behandlung allein aufgrund des transportierten Mediums sollte vermieden werden.

5. Umweltinformationsrechte anpassen

Unterlagen, die in einem Genehmigungsverfahren aus Sicherheitsgründen geschützt werden, dürfen nicht über einen anderen Informationszugang erneut offengelegt werden. Die Änderung des IFG betrifft Bundesstellen und ersetzt weder Anpassungen des Umweltinformationsgesetzes (UIG) noch abgestimmte Regelungen der Länder. Der UIG-Verweis in der vorgesehenen Änderung des Versorgungsrücklagegesetzes schafft ebenfalls keinen allgemeinen Schutz für Infrastrukturinformationen. Anlage 2 enthält einen Vorschlag zur Anpassung des UIG.

Der BDEW fordert deshalb einen eigenständigen und praxistauglichen Schutz umweltbezogener Informationen mit Sicherheitsbezug sowie entsprechende Regelungen im Geodaten- und Landesrecht. Unions- und völkerrechtliche Vorgaben für Umweltinformationen und Öffentlichkeitsbeteiligung sind dabei zu berücksichtigen; verbleibende nationale Spielräume müssen ausgeschöpft werden. Erforderliche Änderungen auf europäischer Ebene sind parallel anzustoßen.

Die laufende Überarbeitung der INSPIRE-Richtlinie sollte genutzt werden, um Geodaten kritischer Infrastrukturen grundsätzlich vom öffentlichen Zugang auszunehmen.

Für Trinkwasserversorgung und Abwasserentsorgung ist dieser übergreifende Ansatz besonders wichtig. Schutzbedürftige Angaben können unter anderem in wasserrechtlichen Verfahren, Geodatenangeboten und Planungsunterlagen enthalten sein. Die Sicherheitsbewertung muss diese Informationswege ausdrücklich einbeziehen. Ein angemessenes Schutzniveau darf weder vom jeweils angerufenen Informationsrecht noch vom Sitz der zuständigen Behörde abhängen.

6. Weitere prioritäre Transparenzpflichten anpassen

Der Entwurf ändert zentrale weitere Regelungsbereiche bislang nicht unmittelbar. Der BDEW fordert, die folgenden Prioritäten in die weiteren Gesetzgebungs- und Vollzugsarbeiten verbindlich aufzunehmen.

Dabei sind insbesondere auch die Transparenz- und Berichtspflichten nach §§ 23b, 23c, 14d und 14e EnWG, §§ 78 und 79 TKG sowie § 3 KraftNAV auf ein sicherheitsverträgliches und für den jeweiligen Zweck erforderliches Minimum zu begrenzen. Öffentliche Informationsbereitstellung und notwendige Meldungen an zuständige Behörden sind differenziert zu bewerten. Unionsrechtliche Spielräume sind auszuschöpfen; erforderliche Änderungen europäischer Vorgaben sind parallel anzustoßen.

Infrastrukturatlas und Leitungsauskünfte

Sicherheitskritische Informationen über Strom-, Gas-, Wasserstoff- und Wasserinfrastrukturen sind vor anlassloser zentraler Vorhaltung und zu weitgehenden Zugriffen zu schützen. Datenpflichten müssen auf den jeweiligen Zweck und tatsächlich erforderliche Informationen begrenzt werden. Vorhandene KRITIS-Ausnahmen sind konsequent anzuwenden und erforderlichenfalls zu erweitern. Dezentrale beziehungsweise bilaterale Auskünfte über Betreiber oder zuständige Kontaktstellen sind zu stärken. Auch bei beschränktem Zugang müssen Berechtigung, Zweck und benötigter Ausschnitt nachvollziehbar sein.

Die Schutzprüfung muss georeferenzierte Angaben zu Leitungen und sonstigen Infrastrukturen ausdrücklich erfassen. Allgemeine Veröffentlichungen und berechtigte, anlassbezogene Leitungs- oder GIS-Auskünfte sind zu unterscheiden. Für notwendige Auskünfte sind Zweckbindung, Berechtigungsprüfung, ein begrenzter räumlicher und sachlicher Ausschnitt sowie geeignete Nutzungsbedingungen und eine nachvollziehbare Dokumentation vorzusehen. Vorhandene regelkonforme Auskunftsprozesse und archivierte Nachweise sollen hierfür nutzbar bleiben.

Das TKG-Änderungsgesetz 2026 und die Gigabit-Grundbuch-Verordnung sind mit dem Transparenz-Anpassungsgesetz abzustimmen und vor ihrem Inkrafttreten so auszugestalten, dass keine zusätzlichen Schutzlücken entstehen. Das Gigabit-Grundbuch bündelt auch Informationen, die Rückschlüsse auf andere kritische Infrastrukturen als Telekommunikationsnetze zulassen. Für zentral vorgehaltene Datenbestände sind deshalb Datenminimierung, erforderliche KRITIS-Ausnahmen und wirksame Zugriffsbeschränkungen vorzusehen.

Für die Anpassung des TKG sind insbesondere die Löschung bereits erhobener Angaben zu gesetzlich bestimmten kritischen Anlagen, Ausnahmen von Datenliefer- und Informationspflichten sowie eine eindeutige Berücksichtigung der Belange der Stromversorgung in Schutzgüterabwägungen vorzusehen. Die Anlage enthält hierzu den von Stromnetz Berlin eingebrachten Regelungsvorschlag für einen zusätzlichen Artikel 3 mit Änderungen zu §§ 1, 78, 79, 136 und 138 TKG in der zugrunde gelegten Entwurfsfassung.

Kapazitätskarten und Verteilernetzentwicklungspläne

Informationen über Anschlussmöglichkeiten und die künftige Versorgung sind für Netzkunden und Investitionen erforderlich. Sie müssen jedoch räumlich und zeitlich so abstrahiert werden, dass keine sicherheitskritischen Rückschlüsse auf einzelne Netzknoten oder betriebliche Engpässe möglich sind. Für Entwicklungs- und Stilllegungsplanungen im Gas- und Wasserstoffbereich sind verständliche Informationen über die Auswirkungen auf Kunden bereitzustellen; detaillierte Netzkarten gehören nur in einen begrenzten, aufgabenbezogenen Zugang. Die Änderung des § 12f EnWG ersetzt diese Anpassungen nicht.

Die Veröffentlichung der Netzanschlusskapazitätskarte nach § 17c EnWG-E („Netzanschlusspaket“) sollte auf die Umspannebene Höchstspannung/Hochspannung sowie auf Hochspannungsnetzgruppen (110 kV) beschränkt werden. Auf eine Veröffentlichung auf Netzebene 4, der Umspannebene Hochspannung/Mittelspannung, sollte aus Gründen des KRITIS-Schutzes verzichtet werden. Eine abstrahierte, gebietsbezogene Darstellung soll die erforderliche Orientierung über Anschlussmöglichkeiten ermöglichen, ohne sicherheitskritische Detailinformationen zu Standorten, Kapazitäten und Netzstrukturen offenzulegen. Damit wird der im Referentenentwurf unter IV. „Alternativen“ angelegte Prüfauftrag konkretisiert.

Zugleich darf der Zugang zu Informationen, die Anschlusspetenten für konkrete Erzeugungs-, Speicher- oder Elektrolysevorhaben benötigen, nicht unverhältnismäßig erschwert werden. Für diese Fälle ist ein geregeltes, fristgebundenes Auskunftsverfahren mit Berechtigungsprüfung und Vertraulichkeitsverpflichtung vorzusehen.

Die niederländische Capaciteitskaart kann als Vergleichsbeispiel für eine gebietsbezogene Darstellung in diese Prüfung einbezogen werden. Ihre Übertragbarkeit auf die vorgeschlagene Beschränkung der Veröffentlichungsebenen ist gesondert zu bewerten.

Die Überprüfung muss neben den Netzausbauplänen der Verteilernetzbetreiber nach § 14d EnWG und den zugrunde liegenden Regionalszenarien auch die Netzentwicklungsplanung für Strom nach §§ 12a und 12b EnWG sowie für Gas und Wasserstoff nach §§ 15a ff. EnWG umfassen. Öffentlich bereitzustellende Informationen sollten, soweit rechtlich möglich, den Ausbaubedarf und geeignete räumliche Korridore darstellen, ohne sicherheitsrelevante technische Detailparameter oder konkrete Trassenverläufe offenzulegen. Erforderliche Anpassungen unionsrechtlicher Vorgaben sind parallel anzustoßen.

Ausschreibungs- und Vergabeverfahren

Das Vergaberecht muss sicherheitsrelevante Infrastrukturinformationen ausdrücklich schützen. Erforderlich sind abgestufte Offenlegungsmodelle: Öffentliche Bekanntmachungen enthalten die für Wettbewerb und Orientierung notwendigen Angaben. Sensible Details sollten erst nach Prüfung der Berechtigung und gegen angemessene Vertraulichkeitsverpflichtungen gegenüber einem möglichst frühzeitig eingeschränkten Teilnehmerkreis bereitgestellt werden. Verstöße gegen Vertraulichkeitsverpflichtungen sind durch wirksame und verhältnismäßige Sanktionen abzusichern. Hierzu sind gesetzliche Grundlagen für spürbare Vergabesperren oder entsprechende Ordnungswidrigkeitstatbestände vorzusehen.

§ 41 Abs. 1 SektVO regelt, dass im Vergabeverfahren von Anfang an alle Informationen veröffentlicht werden müssen. § 41 Abs. 4 SektVO regelt weiter, dass der Auftraggeber festlegt, welche Maßnahmen er zum Schutz der Vertraulichkeit von Informationen anwendet. Das sind aktuell vor allem Vertraulichkeitsvereinbarungen, die wiederum mit Vertragsstrafen (Pönalen) verbunden sind. Eine solche Festlegung ist für den Auftraggeber bislang aber freiwillig.

Wichtig wäre, dass der Auftraggeber frühzeitig, schon im Verdachtsfall, die Möglichkeit erhält, einem Bieter Informationen vorzuenthalten und ihn vom weiteren Verfahren auszuschließen, selbst wenn dieser bereit ist, eine Vertraulichkeitsvereinbarung zu unterzeichnen. Denn Pönalen und selbst Vergabesperren haben keine wirkliche Abschreckungswirkung, wenn der Bieter die Informationen bereits erhalten hat.

Der BDEW fordert daher, dass ein Bieter im Verdachtsfall schon frühzeitig ausgeschlossen werden kann. Der Katalog des § 107 Abs. 2 GWB, wonach das Vergaberecht gar nicht erst angewendet werden muss, wenn der Verdacht besteht, dass sicherheitsrelevante Interessen der Bundesrepublik betroffen sind, müsste entsprechend um Beschaffungen erweitert werden, die kritische Infrastrukturen betreffen.

Darüber hinaus darf ein Auftraggeber nicht allein deshalb zur Öffnung eines Auftrags für den Wettbewerb verpflichtet werden, weil er den beteiligten Unternehmen Vorgaben zum Schutz vertraulicher Informationen machen kann. Denn bereits die Durchführung eines

wettbewerblichen Verfahrens kann erhebliche Sicherheitsrisiken für eine kritische Infrastruktur oder einen kritischen Betrieb begründen.

Der Schutz der Sicherheitsinteressen des Auftraggebers ist nicht zwingend gleichbedeutend mit dem Schutz der öffentlichen Sicherheitsinteressen der Union oder eines Mitgliedstaates. Gerade im Bereich kritischer Infrastrukturen können Sicherheitsinteressen auf der Ebene des konkreten Betreibers bzw. Auftraggebers bestehen, ohne dass sie ohne Weiteres als Sicherheitsinteressen der Union oder des jeweiligen Mitgliedstaates qualifiziert werden können.

Aus Sicht des BDEW sollte nicht allein auf eine formale Einstufung nach den einschlägigen KRITIS-Regelungen abgestellt werden. Vielmehr muss es dem öffentlichen Auftraggeber möglich sein, auch dann besondere Sicherheitsanforderungen zu berücksichtigen, wenn die konkrete Einrichtung oder das konkrete Unternehmen nicht unter den formalen Anwendungsbereich der einschlägigen KRITIS-Regelungen fällt, sich aber aus der konkreten Tätigkeit, den betrieblichen Gegebenheiten, dem Zugang zu Anlagen oder den zu schützenden Informationen ein entsprechender Sicherheitsbedarf ergibt.

Schutzregelungen im GWB, in der Vergabeverordnung und in der Sektorenverordnung sind hierauf zu überprüfen und gezielt weiterzuentwickeln. Die Anforderungen müssen objektiv, diskriminierungsfrei und mit vertretbarem Aufwand erfüllbar sein.

Digitale Plattform Unbemannte Luftfahrt

Bei dipul müssen rechtssichere Flugplanung und die Erkennbarkeit von Betriebsbeschränkungen gewährleistet bleiben. Die öffentliche Darstellung ist auf die hierfür notwendige räumliche und sachliche Detailtiefe zu begrenzen. Sensible Geodaten und Attribute sind zu generalisieren sowie ohne Labelung der Infrastrukturkategorie darzustellen oder ganz auszublenden, soweit sie für diesen Zweck nicht erforderlich sind. Weitergehende Informationen sollten überprüften Berechtigten vorbehalten bleiben. Auch maschinenlesbare Schnittstellen und Massenabrufe sind in das Schutzkonzept einzubeziehen.

Veröffentlichung von Netzstrukturdaten

Auch die Veröffentlichungspflichten für Strom- und Gasnetzbetreiber nach § 23c EnWG sind in die Überprüfung einzubeziehen. Netzstrukturdaten lassen einzeln betrachtet nicht zwingend unmittelbare Rückschlüsse auf die tatsächliche Netztopologie zu, können aber im Zusammenwirken mit weiteren öffentlich verfügbaren Informationen sicherheitsrelevante Rückschlüsse ermöglichen. Die Veröffentlichungspflichten nach § 23c Absatz 1 und 4 EnWG sollten daher auf das unionsrechtlich erforderliche Maß begrenzt und um eine ausdrückliche Schutzregelung ergänzt werden. Sicherheitsrelevante Angaben sind von der Veröffentlichung auszunehmen, wenn sie einzeln oder in Kombination die Sicherheit oder Zuverlässigkeit der Energieversorgung

gefährden können. Soweit europarechtliche Vorgaben entgegenstehen, sollte sich die Bundesregierung auf EU-Ebene für entsprechende Anpassungen einsetzen.

Schutz kritischer Anlagen im Marktstammdatenregister

Für sicherheitsrelevante Daten kritischer Anlagen im Marktstammdatenregister nach § 111e EnWG sollte grundsätzlich von einer besonderen Schutzbedürftigkeit ausgegangen werden, ohne dass Betreiber diese für jede einzelne Angabe zusätzlich nachweisen müssen. Die Schutzregelung des § 15 Absatz 1 Satz 1 Nummer 1 Buchstabe c MaStRV ist entsprechend weiterzuentwickeln. Solche Daten sollten grundsätzlich nicht öffentlich dargestellt werden. Eine räumlich aggregierte Veröffentlichung kommt nur in Betracht, wenn auch unter Berücksichtigung weiterer verfügbarer Angaben keine sicherheitsrelevanten Rückschlüsse auf einzelne Anlagen möglich sind.

Datenumfang der Informationsplattform SMARD

Für die Informationsplattform SMARD nach § 111d EnWG ist zu überprüfen, welche Daten zusätzlich zu bestehenden europäischen Veröffentlichungen tatsächlich erforderlich sind. Der Datensatz sollte auf das erforderliche Maß reduziert werden. Bereits verfügbare Daten sind vorrangig zu nutzen; zusätzliche Meldepflichten, Doppel- und Mehrfacherhebungen, parallele Datenbestände und redundante Veröffentlichungen sind zu vermeiden. In die Prüfung sind auch anlagen- und blockscharfe Erzeugungsdaten einzubeziehen, die nahezu in Echtzeit veröffentlicht werden. Soweit unionsrechtlich zulässig, sollten sie aggregiert oder zeitverzögert dargestellt werden.

Weitere Register und Veröffentlichungswege

Die breitere BDEW-Sammlung zeigt zusätzlichen Prüfbedarf unter anderem beim Marktstammdatenregister, bei Netzschemaplänen, der kommunalen Wärmeplanung sowie bei weiteren Geodaten- und Open-Data-Angeboten. Dabei ist jeweils zu unterscheiden, ob gesetzliche Änderungen erforderlich sind oder bestehende Ausnahmen im Vollzug besser genutzt werden können. Auch neue Informationspflichten müssen bereits vor ihrer Einführung auf Sicherheitsrisiken geprüft werden.

7. Umsetzung und bestehende Veröffentlichungen verbindlich regeln (zu Artikel 8 und zur weiteren Umsetzung)

Das vorgesehene Inkrafttreten am Tag nach der Verkündung ist angesichts des Schutzbedarfs zu begrüßen. Bereits verfügbare Schutzmöglichkeiten müssen zeitnah genutzt werden. Für einen einheitlichen Vollzug sind abgestimmte Anwendungshinweise, klare Ansprechpartner und praktikable Verfahren zur Bewertung sensibler Daten erforderlich. Betreiber sind mit ihrem technischen und betrieblichen Wissen einzubeziehen.

Anwendungshinweise müssen konkretisieren, wie Schutzbedarfsanalysen, Datenklassifizierung, Berechtigungen und externe GIS-Bereitstellungen zusammenwirken. Maßgeblich sind insbesondere die Art der Information, ihre räumliche Genauigkeit, Aktualität und Verknüpfbarkeit sowie der nachgewiesene Aufgabenbedarf der Empfänger. Bereits vorhandene Bewertungen besonders schützenswerter Daten sollen genutzt und bei Bedarf um den Bezug zur Versorgungssicherheit ergänzt werden. Die Einstufung eines Datensatzes ersetzt keine gesonderte Prüfung der für die verarbeitende IT-Infrastruktur geltenden Sicherheitsanforderungen.

Die Begründung spricht die Überprüfung und gegebenenfalls Entfernung bereits veröffentlichter Infrastrukturinformationen an. Ein allgemeines eigenständiges Löschverfahren, das sowohl öffentliche als auch private Stellen erfasst**,** enthält der Entwurf jedoch nicht. Deshalb müssen Zuständigkeiten und Rechtsgrundlagen für eine risikoorientierte Prüfung bestehender Veröffentlichungen konkretisiert werden. Betreiber benötigen einen verlässlichen Weg, sicherheitskritische Veröffentlichungen zu melden und deren Beschränkung überprüfen zu lassen. Bei dringlichen Risiken sollte eine vorläufige Zugriffsbeschränkung bis zur abschließenden Bewertung möglich sein.

Hierfür ist ein ausdrückliches Antragsrecht der betroffenen Betreiber auf Prüfung und, bei Vorliegen der Schutzvoraussetzungen, auf Löschung, Sperrung oder hinreichende Abstraktion sicherheitsrelevanter Veröffentlichungen vorzusehen. Es muss auch Open-Data-Angebote und andere öffentlich zugängliche Datenquellen erfassen. Zuständige Stellen, Bearbeitungsfristen und die Beteiligung der Betreiber sind verbindlich festzulegen. Die Prüfung muss neben Webseiten auch bereitgestellte Dokumente, Downloads und Schnittstellen umfassen. Soweit eine Entfernung oder Änderung geboten ist, sind bekannte weitere amtliche Veröffentlichungsstellen einzubeziehen. Bereits verbreitete Kopien lassen sich nicht vollständig zurückholen; umso wichtiger sind vorbeugende Schutzprüfungen und die Vermeidung erneuter Veröffentlichungen.

Die Bestandsprüfung ist risikoorientiert und mit klarer Verantwortung der jeweils veröffentlichenden Stelle zu organisieren. Vorrang haben aktuelle, detaillierte, georeferenzierte und maschinenlesbare Informationen mit hohem Schutzbedarf. Behörden und Betreiber sollen bekannte Veröffentlichungswege und vorhandene Dokumentationen einbringen können. Eine unbegrenzte Nachforschungspflicht der Betreiber nach sämtlichen fremden Veröffentlichungen ist zu vermeiden. Bestehende, zweckgebundene und dokumentierte Auskunftsverfahren sind gesondert von allgemein zugänglichen Veröffentlichungen zu bewerten.

Der BDEW fordert einen ressortübergreifenden Umsetzungsplan mit benannten Verantwortlichkeiten, konkreten Folgeschritten und nachvollziehbaren Fristen. Dabei ist zu unterscheiden zwischen Regelungen, die in das vorliegende Gesetz gehören, und solchen, für die ein Zeitplan genügt. In dieses Gesetz gehören die Korrektur des IFG-Ausschlussgrundes, das Bundes-

Immissionsschutzgesetz, das Marktstammdatenregister und die Klarstellung zu geplanten Anlagen. Bund und Länder sollten hierfür gemeinsame Maßstäbe entwickeln. Europäische Transparenzvorgaben sind parallel auf Sicherheitsrisiken und Anpassungsbedarf zu prüfen. Wiederkehrende, bereits belastbar dokumentierte Sicherheitsbewertungen müssen nutzbar sein, damit der Schutz nicht durch zusätzliche Nachweisbürokratie erschwert wird. Der Aussage des Entwurfs, der Wirtschaft entstehe kein Erfüllungsaufwand, ist zu widersprechen: Die zusätzliche geheimnisfreie Darstellung nach § 27b Absatz 4 VwVfG verursacht Aufwand in jedem Verfahren. Hierfür sollten standardisierte Muster genügen.

Mit den vorgesehenen Änderungen wird eine wichtige Grundlage gelegt. Entscheidend ist, den Schutz sicherheitsrelevanter Informationen über sämtliche Informationswege hinweg wirksam zu machen und die noch offenen BDEW-Prioritäten zeitnah umzusetzen.

Anlage 1: Regelungsvorschlag zum TKG

Vorschlag für einen zusätzlichen Artikel 3 des Transparenz-Anpassungsgesetzes. Die folgenden Normbezüge und Änderungsansätze folgen der SNB-Eingabe zum TKG-Änderungsgesetz 2026. Der abschließende Änderungsbefehl, die Absatz- und Satzbezüge sowie die unionsrechtliche Zulässigkeit sind mit dem maßgeblichen Stand dieses parallelen Gesetzgebungsverfahrens abzugleichen.

1. Ergänzung der Schutzgüterabwägung in § 1 TKG

Der nach Satz 2 vorgesehene Satz 3 soll wie folgt gefasst werden: „Satz 2 ist in den jeweils durchzuführenden Schutzgüterabwägungen gegenüber den Belangen der Landes- und Bündnisverteidigung und gegenüber den Belangen des § 14d Absatz 10 Satz 1 EnWG nicht anzuwenden.“

Begründung: Die Funktionsfähigkeit der Stromversorgung auf der Verteilernetzebene ist eine Grundvoraussetzung für eine dauerhaft funktionsfähige Telekommunikation. Ihr soll in der beschriebenen Schutzgüterabwägung Rechnung getragen werden.

2. Löschung bereits erhobener Daten nach § 78 Absatz 1 TKG

Nach Satz 3 soll folgender Satz 4 eingefügt werden: „Informationen im Sinne von Satz 2, die bei Infrastrukturen, die durch Gesetz oder aufgrund eines Gesetzes als kritische Anlage bestimmt worden sind, vor Inkrafttreten dieses Gesetzes erhoben wurden, sind von Satz 3 ausgenommen und werden von der zentralen Informationsstelle gelöscht.“

Begründung: Die im TKG-Entwurf vorgesehene Bereitstellung bereits erhobener Informationen im Gigabit-Grundbuch soll für kritische Anlagen ausgeschlossen werden.

3. Ausnahme von Datenlieferpflichten nach § 79 Absatz 2 TKG

Nach Satz 2 soll folgender Satz 3 eingefügt werden: „Soweit Infrastrukturen betroffen sind, die durch Gesetz oder aufgrund eines Gesetzes als kritische Anlage bestimmt worden sind, sind diese von den Verpflichtungen aus Absatz 2 Satz 1 ausgenommen."

Begründung: Der Schutzbedarf kritischer Infrastrukturen soll gegenüber der Erhebung zusätzlicher praxisrelevanter Informationen berücksichtigt werden. SNB verweist hierfür auf die Ausnahmemöglichkeiten für nationale kritische Infrastrukturen nach Artikel 4 Absatz 6 der Verordnung (EU) 2024/1309 sowie auf die Bundestagsentschließung vom 29. Januar 2026.

4. Folgeänderung in § 79 Absatz 4 TKG

§ 79 Absatz 4 Nummer 4 soll gestrichen werden.

Begründung: SNB schlägt dies als Folgeänderung zur Bereichsausnahme nach § 79 Absatz 2 vor.

5. Konkretisierung der Ausnahme in § 136 Absatz 4 TKG

Nummer 3 soll wie folgt gefasst werden: „3. von dem Antrag solche Infrastrukturen betroffen sind, die durch Gesetz oder aufgrund eines Gesetzes als kritische Anlage bestimmt worden sind,"

Begründung: Die Ausnahme von den Informationspflichten nach § 136 Absatz 1 soll für gesetzlich bestimmte kritische Anlagen konkretisiert werden.

6. Ergänzung eines Absatzes 6 in § 138 TKG

Nach Absatz 5 soll folgender Absatz 6 eingefügt werden: „(6) Infrastrukturen, die durch Gesetz oder aufgrund eines Gesetzes als kritische Anlage bestimmt worden sind, sind von den Absätzen 2 bis 5 ausgenommen."

Begründung: SNB hält die ausdrückliche Ausnahme zum Schutz kritischer Infrastrukturen für erforderlich.

7. Anpassung der Artikelzählung

Bei Einfügung des neuen Artikels 3 werden die bisherigen Artikel 3 bis 8 zu den Artikeln 4 bis 9. Dies betrifft das Versorgungsrücklagegesetz (neu Artikel 4), das Gerichtsverfassungsgesetz (neu Artikel 5), das Arbeitsgerichtsgesetz (neu Artikel 6), das Fünfte Buch Sozialgesetzbuch (neu Artikel 7), das Elfte Buch Sozialgesetzbuch (neu Artikel 8) und das Inkrafttreten (neu Artikel 9).

Anlage 2: Regelungsvorschläge zu IFG, BImSchG und VwVfG

Die folgenden Wortlaute sind Arbeitsfassungen. Normstandorte, Absatz- und Satzbezüge sowie die unionsrechtliche Zulässigkeit sind mit dem maßgeblichen Gesetzesstand abzugleichen.

1. Fassung des § 3 Nummer 9 IFG

„9. wenn das Bekanntwerden der Information nachteilige Auswirkungen auf die Sicherheit von Infrastrukturen haben kann, die

a) durch Rechtsvorschrift als kritische Infrastrukturen bestimmt worden sind oder
b) besonders schutzbedürftig zur Wahrung der öffentlichen Sicherheit sind.

Eine besondere Schutzbedürftigkeit nach Buchstabe b ist in der Regel anzunehmen, wenn Informationen über Standorte, Trassen, Bauwerksstruktur, technische Auslegung, Kapazitäten, Abhängigkeiten, Verwundbarkeiten oder Schutzvorkehrungen bestehender, in Errichtung befindlicher oder geplanter Anlagen betroffen sind. Die nachteiligen Auswirkungen auf die Sicherheit der Infrastrukturen können sich auch aus der Zusammenschau mit anderen zugänglichen Informationen ergeben.“

Begründung: Die Regelvermutung übernimmt die Merkmalsliste der Entwurfsbegründung in den Normtext, beseitigt den Widerspruch zwischen Wortlaut und Begründung und erhält eine erkennbare Schadensschwelle.

2. Ergänzung des Bundes-Immissionsschutzgesetzes (neuer Artikel)

„Unterlagen, die Angaben über sicherheitsrelevante Eigenschaften von Infrastrukturen im Sinne des § 30 des Verwaltungsverfahrensgesetzes enthalten, insbesondere über Lage und Anordnung von Anlagenteilen, technische Auslegung, Medienversorgung, Verwundbarkeiten oder Schutzvorkehrungen, sind von der Auslegung und von der Veröffentlichung im Internet ausgenommen. An ihre Stelle tritt eine Darstellung nach § 27b Absatz 4 des Verwaltungsverfahrensgesetzes. Die Genehmigungsbehörde gewährt Personen, die eine mögliche Betroffenheit in eigenen Belangen darlegen, sowie anerkannten Vereinigungen auf Antrag Einsicht in die ausgenommenen Unterlagen; sie kann die Einsicht mit Auflagen zur Vertraulichkeit verbinden. Angaben über Emissionen in die Umwelt bleiben unberührt.“

Begründung: Die Regelung ersetzt die Geltendmachung für einzelne Unterlagen durch eine gesetzliche Regelvermutung, vereinheitlicht den Vollzug und verringert Genehmigungsrisiken. Der Vorbehalt für Emissionsangaben wahrt die Vorgaben der Umweltinformationsrichtlinie.

3. Ergänzung des § 30 VwVfG für geplante Anlagen

„Satz 1 gilt auch für Infrastrukturen, deren Errichtung oder wesentliche Änderung beantragt oder angezeigt ist, wenn sie nach Inbetriebnahme die Voraussetzungen der Nummer 1 oder 2 voraussichtlich erfüllen.“

Begründung: In der Projektphase liegen die detailliertesten Unterlagen vor, während die Anlage noch nicht als kritische Anlage bestimmt ist.

4. Ergänzung von § 8 Absatz 1 UIG (neuer Artikel)

„Zu den bedeutsamen Schutzgütern der öffentlichen Sicherheit nach Satz 1 Nummer 1 gehört insbesondere die Sicherheit von Infrastrukturen, die durch Rechtsvorschrift als kritische Infrastrukturen bestimmt worden sind oder die besonders schutzbedürftig zur Wahrung der öffentlichen Sicherheit sind. Nachteilige Auswirkungen können insbesondere durch die Bekanntgabe von Informationen über Standorte, Trassen, Bauwerksstruktur, technische Auslegung, Kapazitäten, Abhängigkeiten, Verwundbarkeiten oder Schutzvorkehrungen bestehender, in Errichtung befindlicher oder geplanter Anlagen entstehen. Sie können sich auch aus der Zusammenschau mit anderen zugänglichen Informationen ergeben.“

Ansprechpartner

Mathias Böswetter

Fachgebietsleiter KRITIS-, Cyber- und Sicherheitspolitik

+49 30 300199 1526

Mathias.boeswetter@bdew.de