Berlin, 07.04.2026

Angemessene Transparenz schaffen: Sicherheitsrelevante Informationen in der Energie- und Wasserwirtschaft schützen

Die Anschläge auf das Berliner Stromnetz im Januar 2026, aber auch im September 2025, haben eine deutliche Verwundbarkeit kritischer Infrastrukturen in Deutschland aufgezeigt. Sie stehen exemplarisch für eine veränderte geopolitische Lage, in der hybride Bedrohungen, gezielte Sabotageakte und Angriffe auf Versorgungsstrukturen zunehmend Teil sicherheitspolitischer Herausforderungen werden. Auf diese Entwicklungen muss politisch und in enger Abstimmung mit der Branche reagiert werden.

Der Schutz unserer kritischen Infrastrukturen verdient dabei besondere Aufmerksamkeit. Dies gilt insbesondere für die Versorgungsinfrastruktur mit Energie und Wasser sowie für die Entsorgungsinfrastruktur von Abwasser. Sie sind grundlegend für das Funktionieren von Staat, Wirtschaft und Gesellschaft. Störungen, gerade durch gezielte Angriffe, haben weitreichende Folgen für die öffentliche Sicherheit, die wirtschaftliche Stabilität und das tägliche Leben der Bevölkerung.

Die Ereignisse in Berlin haben ein strukturelles Problem unterstrichen: Die angegriffenen Punkte waren im Internet offen auffindbar und vergleichsweise leicht identifizierbar. In vielen Fällen resultiert die öffentliche Verfügbarkeit solcher Informationen aus bestehenden Transparenzpflichten, durch die auch sensible Daten über Infrastrukturstandorte oder -strukturen der Öffentlichkeit zugänglich gemacht werden können.

Gleichzeitig hat sich das Umfeld, in dem solche Informationen genutzt werden können, erheblich verändert. Digitale Dienste – etwa frei zugängliche Kartendarstellungen von Infrastrukturen – erleichtern bereits heute die Identifizierung kritischer Punkte. Hinzu kommen neue technologische Möglichkeiten, insbesondere durch Anwendungen künstlicher Intelligenz, die öffentlich verfügbare, aber gegebenenfalls bislang schwer auffindbare Informationen hochgradig automatisiert zusammenführen und auswerten können. So steigt das Risiko, dass sensible Infrastrukturinformationen gezielt für Angriffe missbraucht werden.

Vor diesem Hintergrund ist eine Neubewertung bestehender Transparenzpflichten erforderlich. Ziel muss es sein, Transparenzanforderungen so auszugestalten, dass sie den veränderten Sicherheitsanforderungen Rechnung tragen. Besonders dringlich erscheint dabei die Überprüfung der nachfolgend aufgeführten Regelungen und Informationspflichten.

Dabei ist zugleich klar: Transparenz gehört zu den grundlegenden Prinzipien eines freiheitlich-demokratischen Systems. Offenheit staatlichen Handelns und Zugang zu Informationen sind zentrale Elemente demokratischer Kontrolle. Gleichzeitig ist jedoch zu berücksichtigen, dass die

Sicherheit kritischer Infrastrukturen – und insbesondere die Versorgungssicherheit bei Energie und Wasser sowie die Funktionsfähigkeit der Abwasserentsorgung – eine grundlegende Voraussetzung für die Stabilität und Handlungsfähigkeit von Staat und Gesellschaft darstellt. Vor diesem Hintergrund gilt es, Transparenz und Sicherheitsinteressen neu auszutarieren.

Neben der dringenden Anpassung bestehender Transparenzpflichten kann und soll die hier aufgeführte, vielfältige Auflistung zudem als klares Argument dafür gelten, neue Transparenzpflichten, die ggf. auch über fachfremde Gesetze eingeführt werden sollen, eingehend zu prüfen. Es braucht ein klares Verständnis, dass Transparenz nicht einmalig, sondern fortwährend mit Sicherheitsaspekten ausbalanciert werden muss.

BDEW-Shortlist der relevantesten Transparenzpflichten

1. Infrastrukturatlas BNetzA

Rechtsgrundlage:

§ 79 TKG (Telekommunikationsgesetz) ist die zentrale Kernnorm für den Infrastrukturatlas: Datenlieferpflichten, Ausnahmen von der Darstellung und Einsichtnahme.

§ 78 TKG regelt die Aufgaben der zentralen Informationsstelle des Bundes (ZIS) als administrative Grundlage.

§ 85 Abs. 2 TKG bildet die Rechtsgrundlage für die Weitergabe von Informationen an andere vertrauliche öffentliche Stellen.

Perspektivisch soll der Infrastrukturatlas beziehungsweise das Gigabit-Grundbuch mit dem TKG-Änderungsgesetz 2026 fortan in den **§§ 78-86 TKG-E** geregelt werden. Hierbei sollen Transparenz- und Datenlieferungspflichten weiter ausgeweitet werden.

Inhalt/Risiko:

Durch den Infrastrukturatlas werden sensible Infrastrukturdaten zentral vorgehalten, wobei die derzeit geltenden Schutz- und Ausnahmeregeln für KRITIS unzureichend sind. Aufgrund der bestehenden erheblichen Cyber- und Sabotagerisiken ist der Status quo nicht tragbar.

Mit dem TKG-Änderungsgesetz sind zudem erweiterte Transparenz- und Datenlieferpflichten geplant. Aus BDEW-Sicht schafft dies zusätzliche Cyber- und Sabotagerisiken für KRITIS, erhöht die Angriffsfläche, verursacht mehr Bürokratie und geht teils über unionsrechtliche Mindestvorgaben hinaus.

Lösungsvorschlag:

Das System soll am Need-to-know-Prinzip ausgerichtet werden: Statt einer anlasslosen zentralen Speicherung sollte eine dezentrale/bilaterale Bereitstellung über die zuständigen Infrastrukturbetreiber bzw. Kontaktstellen erfolgen. Datenpflichten sollten nur für tatsächlich ausbaurelevante Infrastrukturen gelten. Ausnahmen für kritische/sicherheitssensible Infrastrukturen sollten ausgeweitet werden; zusätzlichen Pflichten über die EU-Mindestvorgaben hinaus sollten vermieden werden.

2. „Kapazitätskarte“ (Transparenz bei Netzengpässen)

Rechtsgrundlage:

Die **EU-Strombinnenmarktrichtlinie (Art. 31 Abs. 3)** sieht vor, dass Verteilernetzbetreiber „in transparenter Weise eindeutige Informationen über die für neue Anschlüsse in ihren Betriebsgebieten verfügbare Kapazität“ mit hoher räumlicher Granularität veröffentlichen, allerdings „unter Wahrung der öffentlichen Sicherheit“. Die Bundesregierung plant eine Umsetzung in das deutsche Recht im Zuge des „Netzanschlusspakets“ (§ 17c EnWG-E).

Inhalt/Risiko:

Dem Referentenentwurf zum Netzanschlusspaket zufolge müssen Verteilnetzbetreiber künftig die „auf der Umspannebene von Höchstspannung zu Hochspannung sowie auf der Umspannebene von Hochspannung zu Mittelspannung verfügbaren Netzanschlusskapazitäten auf ihrer jeweiligen Internetseite auf einer geografischen Karte“ veröffentlichen und monatlich aktualisieren. Ein hoher Detailgrad dieser Karten würde gezielte Störungen erheblich erleichtern.

Lösungsvorschlag:

Der Gesetzgeber sollte im kommenden Gesetzgebungsverfahren dringend auf eine Verpflichtung zur Veröffentlichung feingranularer Informationen verzichten. Informationen zu Netztopologien und Engpässen sollten räumlich und zeitlich abstrahiert dargestellt werden, sodass keine Rückschlüsse auf besonders kritische Standorte möglich sind.

3. Verteilernetzentwicklungsplanung (Erdgas/H2)

Rechtsgrundlage:

Wasserstoff- bzw. Erdgasverteilnetzbetreiber müssen laut **Art. 56 EU-Gasbinnenmarktrichtlinie** künftig „Entwicklungspläne“ für Wasserstoffnetze bzw. „Stilllegungspläne“ für Erdgasnetze veröffentlichen. Das Gesetzgebungsverfahren zur Übertragung in deutsches Recht beginnt voraussichtlich noch im März 2026.

Inhalt/Risiko:

Der Referentenentwurf sieht eine verpflichtende Veröffentlichung von „Verteilernetzentwicklungsplänen“ auf den Websites der Betreiber von Erdgas- und/oder Wasserstoffverteilnetzen vor (§ 16b-e EnWG-E). Die Veröffentlichung muss „einfache und verständliche Informationen über den Inhalt des jeweiligen Verteilernetzentwicklungsplans und dessen potenzielle Auswirkungen für Haushaltskunden“ enthalten. Wie bei den Kapazitätskarten im Strombereich gilt: Ein hoher Detailgrad dieser Karten würde gezielte Störungen erheblich erleichtern.

Lösungsvorschlag:

Auch hier sollte der Gesetzgeber im Zuge der Umsetzung in deutsches Recht auf eine Pflicht zur Veröffentlichung feingranularer Netzkarten verzichten und den Zugang auf einen ausgewählten Berechtigtenkreis begrenzen.

4. Genehmigungs- und Zulassungsrechte von Energie- und Wasserinfrastrukturen

Rechtsgrundlage:

- **§ 71 EnWG** (Energiewirtschaftsgesetz)**, § 30a NABEG** (Netzausbaubeschleunigungsgesetz Übertragungsnetz) – Regelungen zum Schutz von Betriebs- oder Geschäftsgeheimnissen im Planfeststellungsverfahren im Bereich Energieleitungen sowie Anlagen wie Umspann- und Schaltanlagen.
- **§ 10 BImSchG** (Bundes-Immissionsschutzgesetz), **§§ 4, 10, 11a der 9. BImSchV** (Verordnung über das Genehmigungsverfahren) – Veröffentlichungspflichten und Schutz von Betriebs- und Geschäftsgeheimnissen in immissionsschutzrechtlichen Genehmigungsverfahren unter anderem für Anlagen der Energiewirtschaft.
- **§§ 19, 23 UVPG** (Gesetz über die Umweltverträglichkeitsprüfung) – Aufnahme/Schärfung eines eigenständigen Geheimnisschutzes für UVP-relevante Unterlagen und Beteiligungsunterlagen.
- **§ 15 Abs. 3 ROG** (Raumordnungsgesetz) – Erweiterung des Schutzes von Betriebs- und Geschäftsgeheimnissen um den Schutz kritischer Infrastrukturen

Inhalt/Risiko:

Zum Schutz Kritischer Infrastrukturen (KRITIS) ist ein wirksamer und praxistauglicher Geheimnisschutz in Genehmigungs-, Planfeststellungs- und sonstigen Zulassungsverfahren dringend erforderlich. In diesen Verfahren werden regelmäßig **Unterlagen mit hohem Detailgrad** offengelegt (insbesondere im Rahmen öffentlicher Auslegung und Anhörungen, zunehmend über Internetportale). Soweit Informationen die physische oder IT-bezogene

Sicherheit gefährden und insbesondere die Planung oder Durchführung von Angriffen erleichtern können, müssen sie von Auslegungs- und Veröffentlichungspflichten ausgenommen bzw. nur in sicherheitsverträglicher Form zugänglich gemacht werden. Ziel ist es, operative Angriffsflächen zu vermeiden, ohne den Kern der Öffentlichkeitsbeteiligung und Verfahrensfairness auszuhöhlen. Bei der Ausgestaltung der Regelungen muss zudem darauf geachtet werden, dass der Schutz nicht durch überzogene Darlegungs- oder Nachweisanforderungen faktisch leerlaufen darf. Zudem muss klargestellt sein, dass auch die sicherheitsbezogene Begründung und etwaige Nachweise selbst dem Geheimnisschutz unterfallen können, um nicht über eine Begründungspflicht indirekt zur Preisgabe sensibler Details zu verpflichten.

Lösungsvorschlag:

Damit der Geheimnisschutz in Genehmigungsverfahren **rechtssicher und bundeseinheitlich** wirkt, sind neben der Neuregelung im Verwaltungsverfahrensgesetz **insbesondere die oben genannten genehmigungsrechtlichen Vorschriften** anzupassen bzw. zu ergänzen, um sicherheitsrelevante KRITIS-Informationen von Auslegung, Anhörung und Internetveröffentlichung auszunehmen oder abgestuft zu behandeln.

5. Informationszugangsrechte und Umweltinformationsrechte

Rechtsgrundlage:

Informationszugangs- und Auskunftsrechte nach dem **Informationsfreiheitsgesetz (IFG),** den **Informationsfreiheitsgesetzen** der Länder sowie dem **Umweltinformationsgesetz (UIG)**.

Inhalt/Risiko:

Informationszugangsrechte müssen so fortentwickelt werden, dass sie den Schutz von KRITIS nicht unterlaufen. Denn selbst wenn Unterlagen im Genehmigungsverfahren teilweise geschwärzt oder nicht öffentlich ausgelegt werden, können identische oder vergleichbare Inhalte über nachgelagerte Informationszugangsansprüche erneut offengelegt werden. Deshalb ist es erforderlich, dass Informationen, die die Sicherheit von KRITIS gefährden oder Angriffe erleichtern können, **verlässlich** von Herausgabe- und Veröffentlichungspflichten ausgenommen werden – einschließlich Transparenz- und Open-Data-Kontexten, Datenlieferpflichten sowie behördlicher proaktiver Veröffentlichungen.

Lösungsvorschlag:

Dringend anzupassen sind insbesondere:

- **IFG** (Informationsfreiheitsgesetz): Ergänzung von § 6 IFG um eine Ausnahme für sicherheitsrelevante KRITIS-Informationen von der Veröffentlichungspflicht. Entsprechende

Regelungen sind auch in den **Informationsfreiheitsgesetzen und den Transparenzgesetzen (vgl. z.B. Rhl-Pf) der Länder** aufzunehmen.

- **UIG** (Umweltinformationsgesetz): § 9 Abs. 1 S. 4 UIG sollte ergänzt werden, um sicherzustellen, dass auch umweltbezogene Informationen mit KRITIS-Sicherheitsbezug in geeigneter Weise geschützt werden können (einschließlich abgestufter Zugänglichmachung, Schwärzungen, ggf. restriktiver Einsichtnahme).

6. Ausschreibungs- und Vergabeverfahren

Rechtsgrundlage:

Das Vergaberecht verpflichtet öffentliche Auftraggeber zur Transparenz und Gleichbehandlung der Bieter. Diese Grundsätze erfordern insbesondere, dass der Auftragsgegenstand in Bekanntmachungen und Vergabeunterlagen hinreichend klar und vollständig beschrieben wird. **§ 41 VgV/SektVO** normiert dabei die Pflicht zur uneingeschränkten, direkten und kostenlosen Bereitstellung der Vergabeunterlagen, während **§ 5 VgV/SektVO** den Schutz vertraulicher Informationen – insbesondere von Betriebs- und Geschäftsgeheimnissen der Unternehmen – sicherstellen soll. Die bestehenden Vorschriften sind jedoch primär auf die Sicherung des Wettbewerbs ausgerichtet und enthalten keine ausdrücklich auf sicherheitsrelevante Informationen zugeschnittenen Schutzmechanismen.

Inhalt/Risiko:

Aus der Pflicht zur Veröffentlichung ergibt sich ein Spannungsverhältnis zwischen Transparenz und Sicherheitsinteressen. Insbesondere bei sicherheitsrelevanten Beschaffungsvorhaben – etwa im Bereich kritischer Infrastrukturen oder IT-Systeme – können Vergabeunterlagen detaillierte Informationen über Systemarchitekturen, Schutzmaßnahmen oder bestehende Schwachstellen enthalten. Diese Informationen können von Dritten missbraucht werden, um Angriffe vorzubereiten oder ein umfassendes Lagebild sensibler Infrastrukturen zu erstellen. Die bestehenden Geheimschutzregelungen greifen hierbei nur eingeschränkt: **§ 5 VgV/SektVO** schützt vor allem die Interessen der Bieter, während **§ 41 VgV/SektVO** zwar eine differenzierte Bereitstellung ermöglicht, jedoch keine klaren Vorgaben zum Umgang mit sicherheitskritischen Informationen enthält. Zudem entsteht das Risiko bereits durch die Veröffentlichung selbst, sodass nachgelagerte Schutzmechanismen nur begrenzt wirksam sind.

Lösungsvorschlag:

Zur besseren Bewältigung dieses Spannungsverhältnisses sind gezielte Anpassungen erforderlich. Zunächst sollte eine klar definierte Kategorie sicherheitsrelevanter Informationen im Vergaberecht eingeführt werden, verbunden mit spezifischen Schutzvorschriften. Darüber hinaus sollten abgestufte Offenlegungsmodelle etabliert werden, bei denen sensible

Inhalte erst in späteren Verfahrensphasen oder nur gegenüber einem begrenzten Bieterkreis offengelegt werden. Ergänzend sollte der Erforderlichkeitsmaßstab für die Bereitstellung von Vergabeunterlagen konkretisiert werden, um Auftraggebern mehr Rechtssicherheit zu geben. Eine stärkere Verzahnung mit spezialgesetzlichen Sicherheitsregelungen, insbesondere im Bereich kritischer Infrastrukturen, ist erforderlich.

7. Nationale Transparenzplattform und Informationsplattform (HEDWIG)

Rechtsgrundlage: **§ 111g EnWG**

Inhalt/Risiko:

Vorgesehen sind die Einrichtung und der Betrieb einer nationalen Transparenzplattform mit energiewirtschaftlichen Daten durch die BNetzA bis spätestens 29.12.2026. Bereitgestellt werden sollen aktuelle Informationen insbesondere zur Erzeugung von Elektrizität, der Last, der Menge der Im- und Exporte von Elektrizität, der Verfügbarkeit von Netzen und von Erzeugungsanlagen sowie zu Kapazitäten und der Verfügbarkeit von grenzüberschreitenden Verbindungsleitungen.

Das Risiko besteht insbesondere darin, dass sich in Kombination mit Standortinformationen, historischen Lastflüssen oder Marktdaten Rückschlüsse auf einzelne Anlagen oder Betreiber ziehen lassen. Damit gehen Gefahren durch Data-Mining, Geo-Engineering und Cybermissbrauch einher. Insbesondere Echtzeitdaten zum Lastfluss innerhalb des Strom-, Gas- oder Wasserstoffnetzes stellen nicht nur ein Betriebsgeheimnis, sondern auch ein gesellschaftliches Sicherheitsrisiko dar, wenn Dritte Zugriff auf diese Echtzeitdaten (viertelstündige Werte je Netzverknüpfungspunkt) bekommen würden.

Lösungsvorschlag:

Mit Blick auf kritische Infrastrukturen dürfen nach BDEW-Auffassung sensible und sicherheitsrelevante Daten - insbesondere in hoher zeitlicher oder anlagenscharfer Granularität - nicht veröffentlicht werden. Der BDEW plädiert für eine klare Schutzabgrenzung und eine Beschränkung der Datentiefe, um die Sicherheit kritischer Infrastrukturen nicht zu gefährden.

8. Digitale Plattform Unbemannte Luftfahrt (dipul)

Rechtsgrundlage:

VO (EU) 2018/1139, VO (EU) 2019/945, VO (EU) 2019/947, ggf. VO (EU) 2021/664 ff. (U-Space), national ergänzt durch LuftVG und LuftVO. Die Veröffentlichung von Informationen

zu UAS-geografischen Gebieten erfolgt unionsrechtlich vorgegeben und national konkretisiert.

Inhalt/Risiko:

Die dipul dient der zentralen digitalen Bereitstellung von Informationen und Regeln für den Drohnenbetrieb, insbesondere zu UAS-geografischen Gebieten, Betriebsbeschränkungen und geobasierten Planungsinformationen. Ein besonderes Risiko entsteht, wenn sicherheitsrelevante Geodaten und Schutzzonen kritischer Infrastrukturen der Energie- und Wasserwirtschaft in hoher räumlicher und sachlicher Granularität öffentlich und maschinenlesbar verfügbar gemacht werden. Je genauer Lage, Zuschnitt, Schutzumfang und zugrundeliegender Anlass der Beschränkung erkennbar sind, desto eher lassen sich Rückschlüsse auf Standort, Funktion, Schutzwürdigkeit und potenzielle Verwundbarkeiten sensibler Anlagen ziehen. In Kombination mit weiteren frei zugänglichen Informationen kann dies die systematische Ausspähung, Zielidentifikation, Routenplanung und Vorbereitung von Stör-, Sabotage- oder Angriffshandlungen erleichtern. Das Risiko liegt daher nicht in der Veröffentlichung von Betriebsregeln als solcher, sondern in einer über das notwendige Maß hinausgehenden Transparenz sicherheitskritischer Detailinformationen.

Lösungsvorschlag:

Die Veröffentlichung sollte strikt am **Erforderlichkeits**- und **Need-to-know-Prinzip** ausgerichtet werden. Öffentlich bereitgestellt werden sollte nur diejenige Informationstiefe, die für rechtssichere Flugplanung, Geo-Awareness und Regelbefolgung tatsächlich notwendig ist. Sensible Layer sollten räumlich generalisiert, maskiert oder anonymisiert werden, sodass Beschränkungen erkennbar bleiben, ohne kritische Standorte oder deren genaue Schutzlogik offenzulegen. Zudem sollte die Attributtiefe konsequent begrenzt werden; insbesondere sollten keine weitergehenden Angaben veröffentlicht werden, die Rückschlüsse auf Art, Funktion oder besondere Schutzbedarfe einzelner Anlagen zulassen, soweit dies für den Regelungszweck nicht erforderlich ist. Ergänzend empfiehlt sich eine abgestufte Zugriffsarchitektur mit einer öffentlichen Informationsebene und weitergehenden Detailinformationen nur für berechtigte Stellen oder Nutzergruppen. Flankierend sollten technische Schutzmaßnahmen wie Logging, Rate-Limiting, Downloadbegrenzungen und Monitoring von Massenzugriffen vorgesehen werden. Erforderlich ist außerdem eine vorgelagerte Klassifizierung der betroffenen Geodaten nach Schutzbedürftigkeit, um sicherzustellen, dass sicherheitskritische Informationen nicht allein aufgrund digitaler Bereitstellungslogik in zu hoher Detailtiefe offengelegt werden.