

Berlin, 14. Oktober 2026

BDEW Bundesverband
der Energie- und
Wasserwirtschaft e.V.
Reinhardtstraße 32
10117 Berlin
www.bdeu.de

Stellungnahme

zum Verordnungsentwurf zur Informationsübermittlung an und Informationsbereitstellung durch das Gigabit-Grundbuch (Gigabit-Grundbuch-Verordnung)

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, 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

1 Einleitung

Ergänzend zu dem TKG-Änderungsgesetz (Telekommunikationsgesetz), das sich derzeit im parlamentarischen Prozess befindet, hat das Bundesministerium am 14. September 2026 einen Referentenentwurf für eine Verordnung zur Informationsübermittlung an und Informationsbereitstellung durch das Gigabit-Grundbuch vorgelegt (GGV). Die rechtliche Grundlage ergibt sich hierbei aus den §§ 78 bis 86 TKG-E, die das Gigabit-Grundbuch als technisches Datenportal der zentralen Informationsstelle des Bundes ausgestalten. Es zielt darauf ab, die Transparenz über den Ausbau öffentlicher Telekommunikationsnetze zu fördern, indem Informationen zu Infrastrukturen, Netzverfügbarkeit, Bauarbeiten etc. zentral gesammelt werden. Der BDEW dankt für die Möglichkeit zur Stellungnahme zum Entwurf der Gigabit-Grundbuch-Verordnung.

Der Bundesverband der Energie- und Wasserwirtschaft e.V. vertritt über 2.000 Mitgliedsunternehmen im Bereich Strom, Gas, Wasser und Telekommunikation, die zu einem Großteil kritische Infrastrukturen in der Energiewirtschaft betreiben und die Versorgungssicherheit der Bevölkerung sicherstellen. Die Energie- und Wasserwirtschaft hat sich in den vergangenen Jahren vermehrt Sabotage- und Cyberangriffen ausgesetzt gesehen¹. Deshalb hat das Bundeskabinett am 29. Januar 2026 beschlossen, bestehende und anstehende Transparenzpflichten kritisch auf sicherheitstechnische Aspekte prüfen zu wollen². Die kritische Prüfung des vorliegenden GGV-Entwurfs ist vor diesem Hintergrund von besonderer Bedeutung.

Der BDEW unterstützt grundsätzlich das Ziel, den Ausbau öffentlicher Telekommunikationsnetze durch einen verbesserten Informationszugang zu erleichtern. Die damit verbundene Transparenz darf jedoch nicht zu Lasten der Sicherheit kritischer Infrastruktur gehen. Der vorliegende Verordnungsentwurf gewährleistet derzeit nur einen unzureichenden Schutz sicherheitssensibler Infrastrukturdaten. Die geplante zentrale Speicherung und transparente Informationsbereitstellung stellen eine erhebliche Angriffsfläche dar und es entstehen Risiken für die Sabotage von Telekommunikations- und Energienetzen sowie Energieerzeugungsanlagen.

¹ Einschlägige Sabotage- und Cyberattacken von Versorgungsinfrastruktur der letzten Monate waren etwa Turnow-Preilack/Jänschwalde (August 2026), Reutlingen (Juni 2026), Berlin (September 2026, 2025), Grünheide (März 2024).

² Siehe Kommunikation der Bundesregierung zum besseren Schutz der deutschen Infrastruktur ([Infrastruktur besser schützen | Bundesregierung](#)).

Daher fordert der BDEW, dass kritische und besonders schutzbedürftige Infrastrukturen bereits vor der Datenübermittlung ausgenommen und der Umfang der bereitzustellenden Informationen auf das tatsächlich erforderliche Maß begrenzt werden. Dies folgt dem „Need to Know“-Prinzip, wonach der Zugang strikt projekt-, zweck- und personenbezogen ausgestaltet werden sollte. Downloads und Weitergaben dürfen nur ausnahmsweise und unter vollständiger Protokollierung möglich sein. Zudem bedarf es verbindlicher und überprüfbarer Sicherheitsanforderungen für alle Zugangsberechtigten und ihre Auftragnehmer. Zusätzliche Meldepflichten zu Sicherheitsvorfällen sind mit den bestehenden Vorgaben des Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS2-UmsCG) und des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSIG) abzugleichen und Doppelmeldungen zu vermeiden.

2 Meldepflichten mit NIS2-UmsCG und Verhältnismäßigkeit abgleichen

Das BMDS plant mit **§ 4 Abs. 2 GGV** eine zusätzliche und inhaltlich nicht hinreichende **Sicherheitsvorfallmeldepflicht für informationssicherheitsrelevante Vorkommnisse** einzuführen. **Der BDEW lehnt diese zusätzlichen Verpflichtungen, in der derzeitigen Fassung, aufgrund fehlender Erheblichkeitsschwelle, fehlenden Bezugs zu den Meldepflichten nach NIS2-Umsetzungsgesetz und BSIG sowie neuer doppelter bürokratischer Hürden ab.**

Mit dem Meldeportal des BSI (nach NIS2-Umsetzungsgesetz) besteht bereits ein zentraler Meldeweg für erhebliche Sicherheitsvorfälle. Aufgrund knapper personeller Ressourcen in den Unternehmen sollten keine Verpflichtungen eingeführt werden, denselben Vorfall erneut an weitere Behörden und öffentliche Stellen zu melden. Die BNetzA, als Betreiberin der zentralen Informationsstelle des Bundes, sollte vielmehr den Informationsaustausch mit dem BSI sicherstellen. Hierfür müssen die notwendigen behördlichen Zugriffs- und Weiterleitungsprozesse geschaffen werden, damit für einen Vorfall jeweils nur eine Meldung notwendig ist.

Fallen Datenlieferanten nicht unter die Regelung des NIS2-Umsetzungsgesetzes, sollte beachtet werden, dass sich aus dem Bezug auf „Vorkommnisse [...]“, die möglicherweise eine Gefährdung ihrer Informationssicherheit begründen“ weder eine Erheblichkeitsschwelle noch eine Verbindung zum Gigabit-Grundbuch erkennen lässt. Die Regelung könnte nach dem jetzigen Stand ebenso geringfügige Verdachtsfälle und Sicherheitsereignisse ohne mittelbare Relevanz für das Gigabit-Grundbuch umfassen.

Die Vorgaben nach § 4 Abs. 2 **widersprechen zudem dem Grundsatz** eines kohärenten und massenfähigen Meldewesens. Der BDEW hat bereits im Gesetzgebungsverfahren zum NIS2-Umsetzungsgesetz dargelegt, dass Meldepflichten auf erhebliche Sicherheitsvorfälle begrenzt

werden sollten. Daher sollten im GGV ausschließlich Sicherheitsvorfälle erfasst werden, bei denen konkrete Anhaltspunkte für eine erhebliche Beeinträchtigung der Vertraulichkeit oder Integrität der im Gigabit-Grundbuch verarbeiteten Informationen, der hierfür genutzten Benutzerkonten oder der Übertragungsschnittstellen bestehen.

Des Weiteren sollte das BMDS die Vorschriften dringend mit bestehenden Vorgaben des NIS2-Umsetzungsgesetzes und des BSIG abgleichen. **Meldungen an die BNetzA sollten entfallen, soweit der Vorfall bereits dem Bundesamt für Sicherheit in der Informationstechnik (BSI) gemeldet wurde.** Der erforderliche Informationsaustausch ist in diesem Fall zwischen den zuständigen Behörden sicherzustellen.

3 Qualitätsstandards mit „bestmöglicher Auflösung“ kritisch prüfen

Nach **§ 7 Abs. 2 GGV** sind **Geodaten in der „höchstmöglichen Auflösung“ zu übermitteln**. Dies übersteigt deutlich die für konkrete Planungen benötigte Datenbereitstellung und erhöht das mögliche Schadenspotenzial des zentralen Datenbestands.

Die Bereitstellung der Infrastrukturdaten im Gigabit-Grundbuch muss daher bedarfsgerecht abgestuft werden. Für die Planung von Ausbauprojekten sind zunächst nur allgemeine oder abstrahierende Angaben notwendig. **Erst bei einem plausibilisierten konkreten Ausbauvorhaben und exakten Lageinformationen sollten weitergehende Informationen ausschließlich bilateral, zweckgebunden und nach Prüfung der Zugangsberechtigung weitergegeben werden.** Darüber hinaus bedarf es weiterführender Ausnahmeregelungen für Geoinformations- und Leitungsdaten kritischer Infrastrukturen, die in den folgenden Abschnitten dargestellt werden.

4 Festlegung der meldepflichtigen Infrastrukturen

§ 8 GGV in Verbindung mit Anhang 1 legt die meldepflichtigen Infrastrukturen fest. Die **Aufnahme von kritischen und sicherheitssensiblen Infrastrukturen wird durch diese Vorgaben deutlich ausgeweitet**. Dabei geht das BMDS deutlich über die in § 4 Abs. 6 GIA erlaubten Ausnahmen hinaus, wonach ausdrücklich nationale kritische Infrastrukturen oder Teile von diesen vollständig von Informationspflichten ausgenommen werden könnten. Die Vorgaben, die durch das BMDS erlassen werden, sind daher unionsrechtlich nicht zwingend aber stellen erneut einen zusätzlichen bürokratischen Aufwand dar und führen zu einer weiteren zentralen Speicherung sicherheitskritischer Daten.

Die damit verbundenen Sicherheitsrisiken beschränken sich jedoch nicht auf die unmittelbar meldepflichtigen kritischen und sicherheitssensiblen Infrastrukturen. Vielmehr muss auch der **Schutz der von Datenlieferpflichten mittelbar betroffenen und benachbarten kritischen Infrastrukturen** berücksichtigt werden. Auch die Übermittlung einer für sich betrachtet nicht

kritischen Leitung kann sicherheitsrelevant sein, wenn unmittelbar daneben produktive Strom-, Gas-, Wasser-, Fernwärme- oder Telekommunikationsinfrastrukturen verlaufen. Hochauflösende Geodaten können in diesen Fällen Rückschlüsse auf Trassenverläufe, Kreuzungs- und Bündelungspunkte, Übergabepunkte, Redundanzen oder Engstellen ermöglichen.

Darüber hinaus sind von Anlage 1 Tabelle 2 auch Anlagen betroffen, die nicht den öffentlichen Netzen dienen. Die Kategorie „Funkmast“ in der genannten Tabelle erfasst auch Trägerstrukturen nichtöffentlicher Betriebsfunk-, BOS- und IoT-Funknetze der Energie- und Wasserversorger. Obwohl diese Netze nicht dem öffentlichen Gigabitausbau dienen und kein Mitnutzungsbedarf erkennbar ist, würde die Meldung sicherheitssensibler Standorte der Notfall- und Steuerungskommunikation offenlegen. Die nachträgliche Ausnahmeprüfung nach § 9 Abs. 2 und § 10 GGV reicht daher nicht aus, da die Standortdaten zunächst zentral übermittelt würden.

Die Ausnahmeprüfung (siehe auch Punkt 5) darf daher nicht nur auf die isolierte Kritikalität der zu meldenden Infrastruktur abstellen. Sie muss auch Umfeld-, Korrelations- und Kumulationsrisiken erfassen. Besteht ein entsprechendes Rückschlussrisiko, muss die Übermittlung vollständig entfallen oder auf abstrahierte beziehungsweise generalisierte Angaben beschränkt werden. Die Entscheidung hierüber muss zwingend vor der Übermittlung vollständiger Lage- oder Vektordaten erfolgen.

Exakte Lageinformationen sollten ausschließlich bei einem nachgewiesenen konkreten Ausbauvorhaben bilateral, zweckgebunden und nach individueller Prüfung der berechtigten Person bereitgestellt werden. Ein zentraler Download oder eine Weitergabe entsprechender Vektordaten ist für sicherheitssensible Bereiche abzulehnen.

Aus Sicht des BDEW sollten die Datenlieferpflichten auf tatsächlich ausbaurelevante, nicht-KRITIS-Infrastrukturen beschränkt werden, von denen sich keine Rückschlüsse auf benachbarte kritische Infrastruktur ableiten lassen. Kann durch die Bereitstellung der Informationen die öffentliche Sicherheit und Ordnung gefährdet werden, sollte keine Pflicht zur Bereitstellung von Informationen festgelegt werden (analog zu § 6a BSIG). Die gesetzliche Grundlage hierfür kann weiterhin im GGV zugrundeliegenden TKG-ÄndG 2026 verankert werden.

5 Inhalt der Datenlieferung und Verfahren für Ausnahmen

Nach **§§ 9 und 10 GGV** werden sowohl die **Inhalte der Datenlieferungen als auch die möglichen Ausnahmen** ausgeführt. Diese Regelungen sind besonders in Verbindung mit § 8 GGV relevant, sollten kritische Infrastrukturen – anders als sicherheitspolitisch geboten – nicht generell von Datenlieferpflichten an das Gigabit-Grundbuch ausgenommen werden. Daher begrüßen wir im Grundsatz die vorgesehenen Ausnahmeregelungen, diese sind allerdings nicht zufriedenstellend.

Im Falle von Cyberangriffen bietet die zentrale Speicherung von Daten eine erhebliche Angriffsfläche. Die zentrale Übermittlung und Speicherung von Geoinformationsdaten stellen daher ein Risiko für weitere physische Sabotage dar.

Deshalb sollte die vorgesehene **Anhörung der Datenlieferanten bezüglich möglicher Ausnahmen durch die zentrale Informationsstelle bereits vor der Datenübermittlung** durchgeführt werden. Bei einer positiven Entscheidung sollte die Lieferpflicht erlöschen. Eine pauschale Datenlieferung und anschließende Anhörung sehen wir als wenig zielführend an, um den ausreichenden Schutz von Infrastrukturdaten sicherzustellen. Zudem könnte der bürokratische Mehraufwand vermieden werden.

6 Zugangsberechtigungen

Die **§§ 30 – 34 GGV** regeln den **Zugang, Umfang und Download der Informationen des Gigabit-Grundbuchs** und stellen dabei die Vorlage der Projektbeschreibung und Befristung für die Dauer des Projektes als Voraussetzung für den Zugriff. Zudem können auch öffentliche Stellen und Auftragnehmer Gebiets- und Downloadrechte erhalten.

Allerdings brauchen andere Netzbetreiber und öffentliche Stellen nur in wenigen Fällen die exakte geografische Lage von kritischen Versorgungsnetzen. Daher sollte sich das **Sicherheits- und Zugriffskonzept des Gigabit-Grundbuchs strikt nach einem projekt-, zweck- und personengebundenen Need-to-Know-Prinzip** ausrichten. In den wenigen Fällen, in denen die Mitteilung von Informationen zwingend notwendig ist, müssen Daten ohnehin bilateral zwischen den Beteiligten unter Einhaltung professioneller Übertragungs- und Speichermethoden und unter Wahrung der Vertraulichkeit ausgetauscht werden. Daher gilt, dass sicherheitssensible Informationen der zentralen Informationsstelle des Bundes nur Akteuren mit nachweisbarem Interesse zugänglich sein dürfen. Dementsprechend ist auch eine pauschale Erweiterung des Zugangsgebietes bis zu 2,5 Kilometern ab Gebietsgrenze sicherheitstechnisch abzulehnen. Ein **Zugriff auf nicht projektbezogene Infrastrukturinformationen ist vor dem Hintergrund einer größtmöglichen Datenminimierung abzulehnen**.

Gesondert zu betrachten ist **§ 32 Abs. 3 GGV**, wonach **Auftragnehmer für drei Monate Zugang zu Informationen des Gigabit-Grundbuchs** erhalten. Beim Gigabit-Grundbuch sollte grundsätzlich nachvollziehbar sein, wer Infrastrukturen abrufen. Zum Schutz der Infrastrukturdaten sollte eine Vertrauenswürdigkeitsüberprüfung von zugriffsberechtigten Mitarbeitenden und Dienstleistern vorgesehen werden. Hier sollte eine Orientierung an den geltenden NIS2-UmsCG-Vorgaben erfolgen. Daher sollte im GGV verankert werden, dass natürliche und juristische Personen, die auf Informationen durch das Gigabit-Grundbuch zugreifen, eine Zertifizierung nachweisen müssen. Dies würde die gesamtwirtschaftliche Resilienz kritischer Versorgungsstrukturen

erhöhen. Sicherheitsnachweise müssen grundsätzlich vor der Freigabe eines Downloads vorliegen. **Nachweise, die bereits im Rahmen der Sicherheitsprüfungen nach NIS2-UmsCG, BSIG oder IT-Sicherheitskatalogen der BNetzA erbracht wurden, sollten ebenfalls für den Zugang zum Gigabit-Grundbuch anerkannt werden, um Doppelprüfungen zu vermeiden.**

Der vorgesehene Download und Weitergabe an weitere Organisationseinheiten von Vektordaten nach **§ 33 Abs. 2 und 3 GGV** sowie **§ 36 Satz 2 GGV** erhöhen das Risiko einer unkontrollierten Vervielfältigung und Zweckentfremdung. Beides sollte nur **ausnahmsweise, nach zusätzlicher Prüfung und unter vollständiger Protokollierung zulässig** sein.

7 Informationssicherheit, Weitergabe und Löschung

Die **§§ 35 bis 38 GGV** enthalten wichtige **Ansätze zum Schutz der im Gigabit-Grundbuch gespeicherten Informationen**. Angesichts der zentralen und hochauflösenden Zusammenführung sicherheitssensibler Infrastrukturinformationen reichen die vorgesehenen Regelungen jedoch nicht aus. Das Gigabit-Grundbuch kann selbst zu einem herausgehobenen Angriffsziel werden. Daher müssen für die zentrale Informationsstelle des Bundes, die zugangsberechtigten Stellen und deren Auftragnehmer gleichermaßen konkrete, verbindliche und überprüfbare Sicherheitsanforderungen gelten. Erforderlich sind insbesondere ein Rollen- und Rechtekonzept nach dem Least-Privilege-Prinzip, eine starke Authentisierung, die Protokollierung sämtlicher Zugriffe und Downloads sowie regelmäßige unabhängige Sicherheitsprüfungen.

Die **Weitergabe und Löschung zugangsgeschützter Informationen** werden in den **§§ 36 und 37 GGV** geregelt. Aus Sicht des BDEW sollte dies nur an vorab benannte und registrierte Personen, für den konkreten Nutzungszweck und im zwingend erforderlichen Umfang erfolgen. Auftragnehmer und sonstige Empfänger müssen gleichwertige Sicherheitsanforderungen erfüllen. Übermittlung über den gemeldeten Empfängerkreis hinaus, sind zu untersagen. Persönliche Authentisierungs- und Anmeldedaten dürfen nicht weitergegeben werden. Nach Wegfall des Verwendungszwecks müssen sämtliche Kopien gelöscht beziehungsweise technisch dauerhaft einer weiteren Nutzung entzogen werden. Die Löschung muss auch Weitergabeempfänger erfassen, dokumentiert werden und risikobasiert überprüfbar sein.

Die derzeitige Regelung des **§ 40 GGV**, wonach **bestehende Registrierungen und Zugangsberechtigungen** nach dem Inkrafttreten der Verordnung fortbestehen sollen, ist im Grundsatz nachvollziehbar. Aufgrund der Notwendigkeit einer Sicherheitsprüfung der Zugangsberechtigten ist eine uneingeschränkte Fortgeltung abzulehnen. Innerhalb einer kurzen Übergangsfrist sollen die bestehenden Zugangsrechte anhand der neuen Anforderungen geprüft werden. Sollten Dienstleister und Auftragnehmer nicht den notwendigen Sicherheitsanforderungen entsprechen, sollten Zugänge unverzüglich entzogen werden.

Ansprechpartner/Ansprechpartnerin

Richard Kaufmann
Fachgebietsleiter Digitale Konnektivität und
IT-Grundsatzfragen
richard.kaufmann@bdew.de

Frederike Rübsam
Fachgebietsleiterin Cybersecurity und Business
Continuity Management
frederike.ruebsam@bdew.de