Brüssel, 13. Oktober 2025

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

Stellungnahme

zum „Digital-Omnibus“ der EU-Kommission

Versionsnummer: final

Inhalt

2. Allgemeine Bemerkungen zur EU-Digitalgesetzgebung

Die Europäische Kommission wird am 19. November 2025 ein sogenanntes „Omnibuspaket“ für digitalpolitische Rechtsakte („Digital-Omnibus“) veröffentlichen. Damit sollen verschiedene Rechtsakte gezielt angepasst und vereinfacht werden. Dieser Ansatz reiht sich in eine Serie weiterer Omnibuspakete ein, die bereits veröffentlicht wurden (bspw. zur Nachhaltigkeitsberichterstattung) oder noch ausstehen. Die EU-Kommission möchte dadurch die Umsetzung verschiedener Vorgaben erleichtern, Wettbewerbsfähigkeit und Innovationen fördern und größere Kohärenz zwischen verschiedenen Maßnahmen schaffen.

Bisher ist noch nicht bekannt, welche Rechtsakte im Rahmen des Digital-Omnibusses angepasst werden sollen. Der BDEW übermittelt daher mit der vorliegenden Stellungnahme im Rahmen der vorbereitenden Sondierung wichtige Impulse und Anpassungsvorschläge zu potentiell im Rahmen des „Digital-Omnibusses“ aufgegriffenen Rechtsakten aus Sicht der Energie- und Wasserwirtschaft.

Grundsätzlich unterstützt der BDEW das Vorhaben der EU-Kommission zur Regelvereinfachung und hat sich in der Vergangenheit wiederholt auf nationaler wie europäischer Ebene für Bürokratieabbau und allgemeine Regelverschlankung sowie -vereinfachung eingesetzt. Bürokratieabbau ist eine zentrale Voraussetzung, um die Energiewende wirksam voranzutreiben und das große Potential der Digitalisierung in Deutschland wie auch in der restlichen EU zu heben. Hierzu möchte der BDEW als deutscher Spitzenverband der Energie- und Wasserwirtschaft einen Beitrag leisten.

Mit großer Sorge betrachtet der BDEW jedoch den gewählten Zeitpunkt und die hohe Geschwindigkeit, mit welcher der Digital-Omnibus vorangetrieben wird. Viele Rechtsakte der Digitalgesetzgebung sind gerade erst abgeschlossen und unmittelbar in Kraft getreten bzw. befinden sich derzeit in der nationalen Umsetzung. Der geplante Omnibus wird aus unserer Sicht sowohl zu früh als auch zu schnell durchgeführt, um gründlich zu erfolgen und die gewünschten Ergebnisse zu liefern. Für die Unternehmen der Energie- und Wasserwirtschaft ist Planungssicherheit und damit verbunden Innovationsfähigkeit und Sicherheit von oberster Bedeutung. Der Digital-Omnibus in seiner jetzigen Form könnte dies hingegen untergaben.

Die nachfolgenden Vorschläge beziehen sich auf die EU-Digitalgesetzgebung der vergangenen sowie laufenden europäischen Legislatur. In Einzelnen umfassen diese die **KI-Verordnung** und die **Datenschutzgrundverordnung (DSGVO)** sowie **Rechtsvorschriften im Bereich Telekommunikation**. Nicht in den Digital-Omnibus aufgenommen werden sollte nach Auffassung des BDEW allerdings der **Data Act**.

Darüber hinaus kann der BDEW zu diesen und weiteren verwandten Rechtsakten der Digitalgesetzgebung (u. a. kritische Infrastruktur und Cybersicherheit) mit einem längeren Zeithorizont gerne weiterführende und detailliertere Rückmeldung geben.

3. Konkrete Anpassungsvorschläge zu einzelnen Rechtsakten

3.1. Datenverordnung (Data Act)

3.1.1. Allgemeine Bemerkungen

Das europäische Datengesetz schafft eine neue, umfassende Rechtsgrundlage für Datenzugangsrechte, die eine optimierte Systemsteuerung in der Energie- und Wasserwirtschaft sowie vielfältige Angebote für Kundinnen und Kunden. Der BDEW sieht den Data Act als eine große Chance für Europas Datenwirtschaft, um den Zugang zu und die Weiterverwendung von Daten zu verbessern. Klarere rechtliche Rahmenbedingungen stärken die europäische Datenwirtschaft und fördern Innovation sowie Wettbewerb. Gerade im Energie- und Wassersektor kann der Datenaustausch entscheidend dazu beitragen, die digitale und grüne Transformation voranzubringen. Gleichzeitig müssen Datensouveränität, wirtschaftliche Zumutbarkeit und die besonderen Rahmenbedingungen unserer Branche unbedingt berücksichtigt werden. Für Unternehmen ist regulatorische Sicherheit zentral: **Der Data Act sollte daher nicht Gegenstand des geplanten „Digital-Omnibusses“ der EU-Kommission zur Vereinheitlichung der europäischen Digitalgesetzgebung sein**. Eine nachträgliche Umgestaltung des Rechtsrahmens bereits kurz nach dessen Inkrafttreten schafft neue Unsicherheit, verursacht zusätzliche Kosten und hemmt wichtige Investitionen. Rechtliche Klarstellungen und Anpassungen durch Reformen sind ein wichtiger Schritt, müssen jedoch im Sinne des Bürokratieabbaus sorgfältig geprüft und vor allem praxistauglich umgesetzt werden. Entscheidend ist, Datenzugang, Innovation und die Umsetzung der Energiewende nicht gegeneinanderzustellen, sondern intelligent miteinander zu verbinden.

3.2. KI-Verordnung (AI Act)

3.2.1. Allgemeine Bemerkungen

In der Energiewirtschaft kommt künstliche Intelligenz (KI) heute bereits in vielen Bereichen erfolgreich zum Einsatz: Zusätzlich zu generativer KI (z. B. zur Text- oder Bilderstellung) wird künstliche Intelligenz auch zur Vorhersage (z. B. von Einspeisungen oder Preisen), zur Optimierung (z. B. Netzführung) oder zur Erkennung (z. B. Fehlerdiagnose) genutzt. Für die Dekarbonisierung der Energiewirtschaft spielt künstliche Intelligenz damit eine herausgehobene Rolle.

Grundsätzlich ist zu begrüßen, dass es einen rechtlichen Rahmen für die Entwicklung und Nutzung von künstlicher Intelligenz gibt. **Die KI-Verordnung betrifft die Energiewirtschaft als Betreiber kritischer Infrastruktur in besonderem Maße**. Das hochkomplexe Regelwerk trifft auf eine ohnehin bereits stark regulierte Branche und stellt Unternehmen damit vor erhebliche Herausforderungen bei der praktischen Umsetzung der Regelungen. Eine stärkere Berücksichtigung sektorenspezifischer bestehender Regularien könnte mögliche Widersprüche, Unklarheiten auflösen und weiteren Bürokratieabbau bedeuten. Hierfür muss allerdings im Detail und ohne Zeitdruck genauer geprüft werden, wo sektorspezifischer Regelungsbedarf besteht. Gerade mit Blick auf den gewählten Zeitpunkt und -plan des „Digital-Omnibusses“ hat der BDEW diesbezüglich große Bedenken. In der Energiewirtschaft existieren beispielsweise bereits eine Reihe an Regelungen zum sicheren Betrieb technischer Anlagen oder zu Anforderungen an die Versorgungssicherheit.

Viele Anwendungsfälle in der Gas-, Wärme- und Stromversorgung könnten in den Hochrisikobereich fallen. Die rechtliche Komplexität wird durch das Nebeneinander verschiedener Regelwerke verstärkt. Denn parallel zur KI-Verordnung gelten weiterhin DSGVO, Urheberrechts- sowie und Cybersicherheitsanforderungen. Hinzu kommen energiewirtschaftliche Besonderheiten, wie die informatorische Entflechtung bei vertikal integrierten Unternehmen und spezielle Anforderungen an die Versorgungssicherheit.

Aus Sicht des BDEW haben die EU-Gesetzgeber die für die Energie- und Wasserwirtschaft bestehenden rechtlichen Unsicherheiten bisher nicht ausreichend ausgeräumt. Auch die bereits veröffentlichten Leitlinien der Europäischen Kommission haben nicht die notwendige rechtliche Orientierung für Unternehmen geschaffen. Daher droht die Gefahr, dass insbesondere Unternehmen mit begrenzten (finanziellen wie personellen) Ressourcen dazu tendieren, von einer umfassenderen Nutzung von KI-Lösungen in der Energiewirtschaft abzusehen.

Die Europäische Kommission sollte daher genau prüfen, wie der Anteil von Hochrisiko-KI-Systhemen im Sinne der KI-Verordnung minimiert werden kann. Wichtig ist, die Anforderungen der KI-Verordnung an die Energie- und Wasserwirtschaft auf wenige „Leitplanken” zu

reduzieren und dabei gleichzeitig den Schutz von Grundrechten und die Berücksichtigung des Datenschutzes sicherzustellen. Zudem müssen zuständige Behörden in den verschiedenen EU-Mitgliedstaaten gezielt Anreize erhalten, damit sie die Vorgaben der KI-Verordnung sowie die EU-Leitlinien einheitlich und abgestimmt anwenden. Dadurch lassen sich doppelte Bewertungen vermeiden und der Verwaltungsaufwand für Unternehmen verringern, die grenzüberschreitend tätig sind. Besonders wichtig ist dabei, die Rollen und Pflichten von Anbietern und Betreibern klarer und einfacher zu definieren – insbesondere dann, wenn es sich um Unternehmen des gleichen Konzerns handelt, der in mehreren Mitgliedstaaten aktiv ist. Weiterhin findet der Aspekt der Innovationsförderung im Verhältnis zur aktuellen Regulierung nicht ausreichend Berücksichtigung. Europäische KI-Politik sollte noch stärker auf Innovation statt (präskriptive) Regulierung zugeschnitten sein und dieses Missverhältnis korrigieren, um die Potenziale dieser transformativen Technologie in vollem Maße nutzen zu können. Dazu zählt auch eine stärkere und ausdrückliche Open-Source-KI-Modellentwicklung.

3.2.2. Konkrete Anpassungsvorschläge

Artikel 3 Absatz 14 – Definition „Sicherheitsbauteil”

Die Begriffsbestimmung des sogenannten „Sicherheitsbauteils” ist zu unspezifisch und muss konkretisiert werden. Der BDEW fordert daher folgende Klarstellungen:

- Abgrenzung zwischen direkten und indirekten Sicherheitsfunktionen
- Materialitätsschwellen für "Gefährdung von Gesundheit und Sicherheit"
- Unterscheidung zwischen funktionskritischen und sicherheitskritischen Komponenten: KI-Systeme, welche die Funktionsfähigkeit eines Prozesses erst ermöglichen, sind hiervon auszunehmen.

Artikel 3 Absatz 15 – Definition „Sicherheitsfunktion“

In der Praxis besteht die Gefahr, dass unverhältnismäßig viele KI-Anwendungen in kritische Infrastruktur (KRITIS) als Hochrisiko-KI-Systeme eingestuft werden können. Unklar ist vor allem, wie mit KI-Komponenten umzugehen ist, die ausschließlich der Cybersicherheit dienen. Nach aktuellem Wortlaut würden diese auch automatisch als Hochrisiko-KI-Systeme gelten, obwohl sie bei Ausfall nicht zwangsläufig eine physische Gefährdung verursachen. Dies bedarf einer Klärung.

Artikel 6 Erwägungsgrund 55 – Klassifizierungsregeln für KI-Systeme mit hohem Risiko

Es ist notwendig, die Frage der Erheblichkeit einer Störung im Sinne von Erwägungsgrund 55 näher zu bestimmen. Im Erwägungsgrund 55 heißt es: *(…) da ihr Ausfall oder ihre Störung in großem Umfang ein Risiko für das Leben und die Gesundheit von Personen darstellen und zu erheblichen Störungen bei der normalen Durchführung sozialer und wirtschaftlicher Tätigkeiten führen kann (…)“.* Es ist unklar, auf welcher Grundlage die Erheblichkeit von Störung bestimmt werden soll. Es ist daher von entscheidender Bedeutung, dass eine Anpassung des Erwägungsgrunds 55 um folgenden Text ergänzt wird.

Textvorschlag: Ergänzung zu Art. 6 Erwägungsgrund 55
„Erfasst werden danach nur solche Komponenten, deren Ausfälle oder Störungen mit erheblichen Auswirkungen auf die Verfügbarkeit der kritischen Infrastruktur („in großem Umfang“) und die Durchführung sozialer und wirtschaftlicher Tätigkeiten („erhebliche Störungen“) einhergehen, was für eine restriktive Auslegung des Begriffs des Sicherheitsbauteils spricht. Erfasst werden zudem nur Schutzsysteme (…)“.

Artikel 6 Absatz 5 – Leitlinien zur praktischen Umsetzung der KI-Verordnung

Nach Art. 6 Abs. 5 der KI-Verordnung soll die Kommission spätestens zum 2. Februar 2026 Leitlinien zur praktischen Umsetzung und eine Liste praktischer Beispiele für hochriskante KI-Systeme unter besonderer Berücksichtigung von Art. 6 Abs. 3 bereitstellen (u. a. weitere Präzisierung und Nutzung der Leitlinien der Europäischen Kommission zur Definition von KI-Systemen, einschließlich möglicher Einsatzmöglichkeiten von generativer KI). Es ist festzustellen, dass die Abgrenzung von Hochrisiko-Systemen im Einzelfall schwierig ist.

Artikel 25 sowie Artikel 96 Absatz 1 – Leitlinien zu „wesentlichen Veränderungen”

Ein Betreiber, der eine wesentliche Veränderung eines Hochrisiko KI-Systems vornimmt oder ein nicht-riskantes System so verändert, dass es zum Hochrisiko KI-Systeme wird, von nach Art. 25 der KI-Verordnung als Anbieter eingestuft. Diese Einstufung bringt sehr weitgehende Pflichten mit sich, die ein Betreiber im Normalfall nicht erfüllen kann. Die Einstufung kann für Betreiber sehr schwerwiegende Konsequenzen, bis hin zu hohen Bußgeldern, haben. Daher sollte die Kommission unbedingt zügig durch Leitlinien nach Art. 96 Abs. 1 KI-Verordnung für Klärung sorgen, wann im Einzelfall eine „wesentliche Veränderung” des KI-Systems anzunehmen ist, durch die der bisherige Betreiber selbst zum Anbieter wird.

Artikel 57 Absatz 1 – Regulatorische Sandkästen für KI

Gemäß Art. 57 Abs. 1 sollen die Mitgliedstaaten sicherstellen, dass ihre zuständigen Behörden auf nationaler Ebene bis zum 2. August 2026 mindestens einen regulatorischen Sandkasten („regulatory sandboxes“) einrichten sollen. Aus Sicht der deutschen Energiewirtschaft ist dies nicht ambitioniert genug und reflektiert das Missverhältnis von Regulierung und Innovation in der KI-Verordnung. Wir schlagen vor, dass jeder Mitgliedstaat einen KI-Regulierungssandkasten je Sektor einrichten sollte, um möglichst viele Verbesserungspotenziale im Rahmen der KI-Verordnung erschließen zu können.

Textvorschlag: Ergänzung zu Art. 57 Abs. 1

*„Die Mitgliedstaaten stellen sicher, dass ihre zuständigen Behörden auf nationaler Ebene mindestens einen Sandkasten für KI-Regulierung **je Wirtschaftssektor** einrichten, der bis zum 2. August 2026 betriebsbereit sein muss.”*

Artikel 113 – Inkrafttreten und Anwendung

Verschiedene politische Akteure haben eine mögliche Fristverschiebung für die Regelungen der KI-Verordnung vorgeschlagen. Aus Sicht des BDEW ist derzeit zu bezweifeln, dass bis August 2026 alle Rechtsunsicherheiten, insbesondere mit Blick auf die Zertifizierung von Hochrisiko-KI-Systemen, beseitigt werden. Eine Verschiebung der Fristen, vor allem bzgl. der Anforderungen an Hochrisiko-KI-Systeme, würde die Energiewirtschaft daher nicht ablehnend gegenüberstehen. Der BDEW unterstützt insbesondere die Sanktionierung durch Bußgelder aufzuschieben, sofern eine Fristverschiebung nicht möglich ist.

3.3. Datenschutzgrundverordnung (DSGVO)

3.3.1. Allgemeine Bemerkungen

Der BDEW fordert im Sinne einer Vereinfachung und Entbürokratisierung der DSGVO, bei der Ausgestaltung und Anwendung des europäischen Datenschutzrechts einen stärker risikoorientierten Ansatz verbindlich zu verankern. Hintergrund sind folgende fünf Punkte:

- **Fokus auf tatsächlichen Risiken**: Datenschutzanforderungen müssen sich klar an dem Risiko für die Rechte und Freiheiten der betroffenen Personen orientieren, anstatt starre und pauschale Vorgaben zu machen.
- **Entlastung bei geringem Risiko**: Bei Verarbeitungsvorgängen mit nur geringem Risiko sollten Unternehmen von bürokratischen Nachweispflichten entlastet werden. Das reduziert unnötigen Aufwand und stärkt die Wettbewerbsfähigkeit.

- **Konzentration auf kritische Datenverarbeitungen**: Aufsichtsbehörden sollen ihre Prüf- und Kontrolltätigkeiten dort bündeln, wo hohe Risiken bestehen – insbesondere bei sensiblen Daten, großflächiger Überwachung oder automatisierten Entscheidungen mit erheblicher Tragweite.
- **Klarheit und Praxistauglichkeit**: Erwartet werden Leitlinien und Kriterien, die eine nachvollziehbare Bewertung von Risiken ermöglichen. Dadurch können Verantwortliche rechtssicher entscheiden, welche Maßnahmen im jeweiligen Kontext „angemessen“ sind.
- **Stärkung von Innovation und Digitalisierung**: Ein klarer, risikoorientierter Rechtsrahmen unterstützt Unternehmen dabei, neue Technologien verantwortungsvoll einzusetzen, ohne durch unverhältnismäßige Auflagen gehemmt zu werden.

3.3.2. Konkrete Anpassungsvorschläge

Artikel 6 Absatz 2 DSGVO - Rechtmäßigkeit der Verarbeitung in Verbindung mit Art. 85 DSGVO ff Vorschriften für besondere Verarbeitungssituationen

Unternehmen benötigen für den Einsatz von Videoüberwachung mehr Rechtssicherheit, ohne dass die Rechte der betroffenen Personen unangemessen eingeschränkt werden. Die Sicherheitslage hat sich in den vergangenen Jahren spürbar verändert. Kritische Infrastrukturen, sensible Unternehmensstandorte und Einrichtungen sehen sich zunehmend Bedrohungen ausgesetzt – von Vandalismus über organisierte Kriminalität bis hin zu potenziellen Angriffen auf die Versorgungssicherheit. Vor diesem Hintergrund steigt der Bedarf an wirksamen Schutzmaßnahmen. Gleichzeitig sind Unternehmen und Betreiber mit einem akuten Fachkräftemangel im Bereich Sicherheitspersonal konfrontiert. Eine personelle Überwachung ist in der Praxis vielfach nicht leistbar – weder organisatorisch noch wirtschaftlich. Ohne den ergänzenden Einsatz moderner technischer Lösungen droht daher eine erhebliche Schutzlücke. Videoüberwachung stellt in diesem Kontext eine effiziente und unverzichtbare Maßnahme dar, um Sicherheit zu gewährleisten und den Betrieb kritischer Infrastrukturen zuverlässig aufrechtzuerhalten. Dabei ist zu betonen, dass technologische Innovation – von intelligenter Kameraüberwachung bis hin zu automatisierten Zutrittskontrollen – nicht behindert, sondern ausdrücklich ermöglicht werden muss. Nur so können Unternehmen den gestiegenen Anforderungen an Sicherheit, Prävention und Gefahrenabwehr gerecht werden. Ein klarer und rechtssicherer Rechtsrahmen für den Einsatz von Videoüberwachung ist daher unabdingbar.

Textvorschlag: Ergänzung des Art. 6 Abs. 2 DSGVO

*„(2) Die Mitgliedstaaten können spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung in Bezug auf die Verarbeitung zur Erfüllung von Absatz 1 Buchstaben c, **e und f** beibehalten oder einführen, indem sie spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser bestimmen, um eine rechtmäßig und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten, einschließlich für andere besondere Verarbeitungssituationen gemäß Kapitel IX.“*

Textvorschlag: Hinzufügung eines neuen Art. 85 a 1 DSGVO
„Die Mitgliedstaaten können durch Rechtsvorschriften spezifische Regelungen für die Verarbeitung personenbezogener Daten durch Videoüberwachung erlassen, soweit dies erforderlich ist, insbesondere um

a) den Schutz kritischer Infrastrukturen

b) die Gewährleistung von Zutrittskontrollen zu besonders gesicherten Bereichen

c) den Objektschutz bei nachgewiesener erhöhter Gefährdungslage

sicherzustellen.“

Artikel 24 Absatz 1 DSGVO – Verantwortung des Verantwortlichen

Die geltende DSGVO behandelt alle Arten personenbezogener Daten gleich, obwohl das Risiko für die Betroffenen unterschiedlich ausgeprägt ist. Dies führt zu Überregulierung bei geringfügigen Risiken (z. B. berufliche Kontaktdaten) und bindet Ressourcen, die besser für risikoreiche Datenverarbeitungen eingesetzt würden. Durch die Einführung eines ausdrücklich normierten risikobasierten Ansatzes soll die DSGVO praxisgerechter, verhältnismäßiger und innovationsfreundlicher ausgestaltet werden.

Textvorschlag: Nach Abs. 1 DCGVO (der zu Abs. 1a wird) wird folgender Abs. (1b) neu eingefügt:

„(1b) Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen, risikobasiert um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt.“

Beispielsweise ist die Verarbeitung beruflicher Kontaktdaten wie dienstlicher Telefonnummern oder E-Mail-Adressen in der Regel mit einem geringeren Risiko verbunden als die

Verarbeitung privater Kontaktdaten oder sensibler Informationen. Daher können für berufliche Kontaktdaten vereinfachte Pflichten gelten, solange sie ausschließlich zur beruflichen Kommunikation genutzt werden. Das würde den bürokratischen Aufwand auch bei der Zusammenarbeit von Unternehmen hinsichtlich der beruflichen Kontakte (gemeinsame Datenschutzerklärung, Vereinbarung über die gemeinsame datenschutzrechtliche Verantwortlichkeit gemäß Art. 26 DSGVO etc.) reduzieren. Zum Beispiel ist es ein erheblicher Aufwand Auftragsverarbeitungsanträge (AVV) abzuschließen, wenn der Auftragsverarbeiter lediglich den Namen und ggf. eine E-Mail-Adresse als Login-Daten für ein geschäftlich genutztes Tool sieht und darüber hinaus in diesem Tool gar keine personenbezogenen Daten verarbeitet werden. Gleiches gilt für die Aufnahme in das Verzeichnis von Verarbeitungstätigkeiten (VVT). Das umfasst auch eine vereinfachte Verarbeitung von personenbezogenen Daten, die gerade zur Datennutzung bestimmt sind, wie z. B. Visitenkarten oder Kontaktdaten, die von Geschäftspartnern per E-Mail überlassen werden.

Artikel 30 DSGVO - Verarbeitungsverzeichnis / Umfassende Dokumentationspflichten

Jede Datenverarbeitung, auch wenn diese nur ein sehr geringes Risiko aufweist, muss in einem Verarbeitungsverzeichnis umfassend dokumentiert werden. Wünschenswert wäre, wenn bei Verarbeitungen mit nur sehr geringem Risiko die Mindestinhalte deutlich reduziert werden oder darauf verzichtet wird.

Textvorschlag: Hinzufügung eines neuen Art. 30 Abs. 6 DSGVO

„(6) Abweichend von den Absätzen 1 bis 5 kann von der Pflicht zur Führung eines Verzeichnisses abgesehen werden, soweit es sich um Verarbeitungsvorgänge handelt, die nur ein sehr geringes Risiko für die Rechte und Freiheiten natürlicher Personen begründen. Dies gilt insbesondere dann, wenn die Verarbeitung nur in begrenztem Umfang erfolgt, lediglich einen klar abgegrenzten Zweck verfolgt, keine besonderen Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 oder Daten im Sinne des Artikels 10 umfasst.”

Artikel 33 DSGVO - Meldepflicht von 72 Stunden bei Risiko/ Datenschutzverletzungen

Die Meldefrist von 72 Stunden ist sehr kurz bemessen. Die Praxis zeigt, dass in der konkreten Situation (z. B. Hackerangriff) die verfügbaren Ressourcen vielmehr für die Analyse und Ergreifung von Abhilfemaßnahmen benötigt werden. Aufgrund der DSGVO-Vorgaben muss das Bestehen einer Meldepflicht geprüft und ggf. eine Meldung erstellt werden. In Anbetracht der immer komplexeren (technischen) Zusammenhänge ist mehr Zeit erforderlich. Außerdem zeigt die Praxis, dass häufig nur automatisiert standardisierte Rückmeldungen durch die

Behörde erfolgen und keine inhaltliche Auseinandersetzung erfolgt, die den zeitlichen Druck und die Bindung wertvoller Ressourcen erfordert.

Textvorschlag: Anpassung von Art. 33 Abs. 1 DSGVO

*„(1) Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen **7 Werktagen** ~~**72 Stunden**~~, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen **7 Werktagen** ~~**72 Stunden**~~, so ist ihr eine Begründung für die Verzögerung beizufügen.“*

Standardisierung im Datenschutzrecht

Ein weiteres zentrales Anliegen des BDEW ist eine stärkere Standardisierung im Datenschutzrecht. Die Schaffung verbindlicher Standards und Muster durch die Kommission würde die DSGVO für Unternehmen – insbesondere für KMU – erheblich praktikabler machen und gleichzeitig das Datenschutzniveau sichern. Bürokratieabbau, Rechtssicherheit und Effizienzsteigerung lassen sich so in Einklang mit den Grundprinzipien des Datenschutzes erreichen.

- **Einheitliche Standards für VVT und DSFA**

Wünschenswert wäre es, wenn die Bereiche Verzeichnis von Verarbeitungstätigkeiten und Datenschutz-Folgenabschätzung (DSFA) nicht nur vereinfacht, sondern durch einheitliche Standards geregelt würden.

Hierzu regt der BDEW an, die EU-Kommission dazu zu ermächtigen, durch Durchführungsrechtsakte Muster und Vorlagen bereitzustellen, die von Verantwortlichen genutzt werden können. Auch Empfehlungen für Löschfristen persönlicher Daten in standardisierten Konstellationen, z. B. in Bewerbungen oder Personalakten, helfen Verantwortlichen bei der Vereinheitlichung und Entbürokratisierung z. B, auch für Softwarelösungen.

Eine Risikomatrix, wie sie heute bereits vielerorts in der DSFA eingesetzt wird, sollte direkt in der DSGVO verankert werden. Viele Unternehmen haben Probleme, Risiken systematisch zu bestimmen – insbesondere, wenn technische und organisatorische Maßnahmen (TOMs) als risikomindernde Faktoren berücksichtigt werden sollen.

- **Bürokratieabbau durch standardisierte Dokumentationspflichten**

Der Aufwand für Unternehmen lässt sich spürbar reduzieren, wenn vereinfachte Dokumentationspflichten auf der Basis standardisierter Vorlagen eingeführt werden. Denkbar sind Muster für:

- Auftragsverarbeitungsverträge (AVV)
- Technische und organisatorische Maßnahmen (TOM)
- Verträge zur gemeinsamen Verantwortlichkeit
- DSFA und Transfer Impact Assessments (TIA)

Gerade kleinere Unternehmen, die selten DSFA oder TIA durchführen müssen, benötigen klarere und verbindlichere Vorgaben, um diese rechtskonform und effizient umsetzen zu können.

3.4. Telekommunikation

3.4.1. Allgemeine Bemerkungen

Flächendeckende gigabitfähige Telekommunikationsnetze im Festnetz und Mobilfunkbereich sind wesentliche Erfolgsfaktoren für digitale Innovationen, eine erfolgreiche Energiewende und die zukünftige Wettbewerbsfähigkeit Europas. Besonders Berichtspflichten zu Infrastrukturdaten und komplizierte Genehmigungsprozesse stellen dabei erhebliche bürokratische Belastungen dar. Hierdurch wird der schnelle Ausbau der notwendigen digitalen Infrastrukturen unnötig ausgebremst. Eine Vereinfachung und Reduzierungen der Vorgaben sind daher dringend notwendig.

Der BDEW begrüßt daher, dass das Ziel des Bürokratieabbaus und Vereinfachung im Bereich der Telekommunikationspolitik auf europäischer Ebene gleich an mehreren Stellen diskutiert wird. Besonders hervorzuheben ist hierbei – neben dem mit dieser Stellungnahme kommentierten Digital-Omnibus ebenfalls der „Digital Networks Act“, der im Dezember 2025 erwartet wird.

3.4.2. Konkrete Anpassungsvorschläge

Meldepflichten von Geoinformationsdaten auf Notwendigkeit prüfen

Der Europäische Kodex für elektronische Kommunikation (EECC) verpflichtet in Art. 22 zu einer geografischen Datenerhebung, soweit dies für die Aufgaben der nationalen Regulierungsbehörden bzw. anderer zuständiger Behörden und für die Anwendung der Beihilfevorschriften

erforderlich ist. Hieraus ergeben sich eine Reihe sicherheitsrelevanter Risiken, da in der Praxis eine Vielzahl von Stakeholdern die Datensätze einsehen können. Darüber hinaus bezweifelt der BDEW, dass durch die Datenerhebung der Netzausbau beschleunigt wird.

Daher sollte bei weiteren Schritten zum Bürokratieabbau die gesetzlichen Regelungen zur Datenerhebung und -bereitstellung auf ein Mindestmaß beschränkt werden. Zudem ist zu prüfen, ob im Sinne des Schutzes kritischer Infrastrukturen verpflichtende Ausnahmeoptionen eingeführt werden sollten, um die Versorgung der Bevölkerung vor Sabotagen zu schützen. Daten sollten nur sparsam erhoben und zentral gespeichert werden – hierbei gilt es, dass „Need to Know“-Prinzip einzuhalten. Somit sollte angedacht werden, dass statt Infrastrukturdaten lediglich Kontaktpersonen der zuständigen Unternehmen abzufragen sind. Schließlich sind die erhobenen Daten für Bauarbeiten oder Anfragen zur Mitnutzung zu passiven Infrastrukturen nicht aktuell oder detailliert genug. Daher würde es ausreichen, lediglich Kontaktinformationen, statt unpassender Daten bereitzustellen. Die Eigentümer oder Betreiber der nutzbaren Infrastruktur geben auf Nachfrage freiwillig Informationen an Interessenten heraus und halten dabei hohe Sicherheitsstandards ein.

Vereinfachung von Vorgaben aus der Gigabitinfrastrukturverordnung

Im Rahmen der Umsetzung der Gigabitinfrastrukturverordnung (GIA) begrüßt der BDEW die Möglichkeit einer Zugangsverweigerung zu physischer Infrastruktur, da anderenfalls das Risiko für volkswirtschaftlich schädlichen Doppelausbau unnötig steigt. Hierdurch würden Investitionen entwertet und der weitere Glasfaserausbau deutlich verlangsamt.

Die derzeitigen Ausnahmeregelungen des Art. 3 Abs. 6 GIA bestimmen, dass Eigentümer physischer Infrastruktur den Zugang zu bestimmten physischen Infrastrukturen nur verweigern können, wenn vom selben Netzbetreiber tragfähige Alternativen für den diskriminierungsfreien offenen aktiven Zugang zu Gigabitnetzen auf Vorleistungsebene bereitgestellt werden. Zudem knüpft sich die Vorgabe an die Bedingung, dass das Aufbauprojekt des antragstellenden Betreibers das gleiche Gebiet abdecken muss.

Nach Auffassung des BDEW ist diese Regelung zu eng gefasst und greift in einigen wichtigen Anwendungsfällen nicht. Fälle, bei denen ein Open Access-Produkt nicht von dem Besitzer der Infrastruktur – aber zum Beispiel von einem Schwesterunternehmen angeboten werden kann – werden derzeit von der Regelung ausgenommen und stellen keine ausreichenden Ablehnungsgründe dar. Daher sollte eine Erweiterung der Ausnahmegründe stattfinden.

Textvorschlag: *„Die Mitgliedstaaten können vorsehen, dass die Netzbetreiber und öffentlichen Stellen, die Eigentümer physischer Infrastrukturen sind oder diese kontrollieren, den Zugang zu*

bestimmten physischen Infrastrukturen verweigern können, wenn ***~~vom selben Netzbetreiber oder derselben öffentlichen Stelle~~*** *tragfähige Alternativen für den diskriminierungsfreien offenen aktiven Zugang zu VHC-Netzen auf der Vorleistungsebene bereitgestellt werden, sofern* ***~~beide~~*** *folgende Bedingungen erfüllt* ***~~sind~~ wird****:*

a) Diese tragfähigen Alternativen für den Zugang auf der Vorleistungsebene werden zu fairen und angemessenen Bedingungen, einschließlich des Preises, angeboten;

b) ***~~das Aufbauprojekt des antragstellenden Betreibers betrifft das gleiche Abdeckungsgebiet und~~*** *es gibt in dem Abdeckungsgebiet kein anderes Glasfasernetz für den Anschluss an Räume von Endnutzern.*

Dieser Absatz gilt nur für diejenigen Mitgliedstaaten, in denen diese oder eine gleichwertige Verweigerungsmöglichkeit am 11. Mai 2024 nach Maßgabe des mit dem Unionsrecht im Einklang stehenden nationalen Rechts angewandt wird.“