Deutscher Verein des
Gas- und Wasserfaches e.V.

www.dvgw.de

# STELLUNGNAHME

**vom 24. August 2023 zu**

# Entwurf eines Gesetzes zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen (KRITIS-Dachgesetz – KRITIS-DachG)

DVGW Deutscher Verein des
Gas- und Wasserfaches e.V.

**Ansprechpartner**
**Peter Frenz (Wasser)**
**Hiltrud Schülken (Gas)**
Josef-Wirmer-Straße 1-3
D-53123 Bonn
Tel.: +49 228 9188-654, +49 228 9188-905

E-Mail: peter.frenz@dvgw.de; hiltrud.schuelken@dvgw.de

## Zusammenfassung

Der DVGW e. V. begrüßt grundsätzlich den Entwurf eines Gesetzes zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen (KRITIS-DachG) vom 17. Juli 2023.

Vor dem Hintergrund der geopolitischen Zeitenwende und der damit eingehenden Risiken von Sabotageakten und Cyberbedrohungen muss der **rechtliche Rahmen für den Schutz der Kritischen Infrastrukturen ganzheitlich geregelt und weiter fortgeschrieben werden**. Nur durch einen umfassenden „All-Gefahren-Ansatz“, der Risiken aus dem Cyberraum, dem Informationsraum und dem physischen Raum ganzheitlich berücksichtigt, kann die Resilienz der Kritischen Infrastrukturen in Deutschland erhöht werden. **Dafür sieht der DVGW in dem vorliegenden Entwurf des KRITIS-DachG grundsätzlich einen geeigneten Rahmen.**

Der DVGW fasst seine Kernforderungen wie folgt zusammen:

1. Die Gesetzgebungskompetenz des Bundes für das KRITIS-DachG basiert auf Art. 74 Abs. 1 Nr. 11 Grundgesetz (Recht der Wirtschaft). Damit ist das KRITIS-DachG ein Wirtschaftsgesetz und kein Sicherheitsgesetz. Entsprechend sollte es der Wirtschaft nur Leitplanken zur Erhöhung der Resilienz von Kritischen Infrastrukturen geben, die durch die Wirtschaft mittels eines risikobasierten Ansatzes in geeignete Maßnahmen übersetzt und schließlich umgesetzt werden können.

   Hieraus ergibt sich u.a. die Maßgabe der weitestgehenden Nutzung von bewährten Strukturen der Technischen Selbstverwaltung (Technische Regelsetzung), die das Optimum zwischen Sicherheit, Hygiene, Umweltschutz und Wirtschaftlichkeit fokussieren.

   Mit Blick auf bestehende bewährte Mechanismen und Strukturen der technischen Selbstverwaltung in den einzelnen Sektoren, fordert der DVGW, den Grundsatz der eigenverantwortlichen Umsetzung von Resilienzmaßnahmen der Betreiber im KRITIS-DachG zu verankern und somit zu stärken. Der DVGW begrüßt ausdrücklich die Möglichkeit, spezifische Resilienzstandards zur Gewährleistung der Anforderungen nach § 11 (5) KRITIS-DachG vorschlagen zu dürfen, wie es für die IT-Sicherheit mit dem B3S Wasser/Abwasser (z. B. DVGW W 1060) bereits verankert ist. Der DVGW unterstützt mit seiner Technischen Regelsetzung die Unternehmen der Gas- und Wasserversorgung bereits heute in der Aufstellung und Umsetzung von Resilienzmaßnahmen. Zum Vorteil der vielen Querverbundunternehmen in Deutschland entsteht das DVGW-Regelwerk – wo sinnvoll – abgestimmt zwischen allen Medien, und auch in intensiver Abstimmung mit den Regelsetzern für andere kritische Infrastrukturen, wie Strom (VDE-FNN), Abwasser (DWA) und Fernwärme (AFGW). Als Beispiel sei hier das Technische Sicherheitsmanagement (TSM) und die Kooperation zum physischen Schutz von kritischen Anlagen genannt. Diese Herangehensweise entspricht dem sektorenübergreifenden Ansatz des KRITIS-DachG.
   Der bereits durch eine Bundesbehörde etablierte Standards für den Informationssicherheitsschutz (IT-Sicherheitskatalog) für die Gas- und Energieunternehmen sollte bei der Festlegung von Mindestanforderungen beim physischen Schutz von kritischen Anlagen und Komponenten nicht als Blaupause gelten. Vielmehr ist hier die Festlegung von Mindeststandards durch die Branche im Sinne der Technischen Selbstverwaltung das zielführende Modell. Der DVGW entwickelt derzeit in Anlehnung an DVGW W 1050 ein Technisches Regelwerk für den physischen Schutz von gastechnischen Anlagen.

2. Unnötiger Bürokratismus und Planungsunsicherheit - etwa durch Doppelregistrierungen oder Beschaffungsvorbehalte bei kritischen Komponenten - sind unbedingt zu vermeiden, um den optimalen Einsatz der personellen und finanziellen Ressourcen im Sinne der Resilienz zu ermöglichen.

3. Der DVGW unterstreicht die Notwendigkeit für eine **enge Verzahnung von KRITIS-DachG und NIS-2-Umsetzungsgesetz (NIS2UmsuCG)**. Eine nahtlose Verzahnung ist die Voraussetzung für eine effiziente, umsetzbare und wirtschaftlich abbildbare Gesetzgebung zum Schutz Kritischer Infrastrukturen und muss insbesondere bei der Ausgestaltung der noch zu erlassenden Rechtsverordnungen in den jeweiligen Sektoren nach § 15 KRITIS-DachG beachtet werden. Diese sollten sektorenspezifisch zugeschnitten und abgegrenzt sein sowie auf bereits bestehende gesetzliche Regelungen der jeweiligen Sektoren aufbauen.

4. Der DVGW begrüßt die vorgesehene Anerkennung von Risikoanalysen/-bewertungen und Zertifikaten, die an anderer Stelle von Betreibern kritischer Anlagen bereits gefordert werden. In diesem Kontext weist der DVGW für den Sektor Wasser auf die branchenspezifischen Sicherheitsstandards (technische Regeln) des DVGW für technische Sicherheit (DVGW G/W 1000), den physischen Schutz (DVGW W 1050) und für IT-Sicherheit (DVGW W 1060) hin. Sie sollten im Sinne der weiteren spezialgesetzlichen Regelungen nach § 5 KRITIS-DachG als Grundlage für Risikoanalysen und -bewertungen der Betreiber kritischer Anlagen nach § 10 KRITIS-DachG sowie für die Resilienzmaßnahmen und ihrer Nachweise in Form von Zertifikaten nach § 11 KRITIS-DachG anerkannt werden.
   Bestehende branchenspezifische Sicherheitsmanagementsysteme (Technisches Sicherheitsmanagement TSM des DVGW) und Nachweisverfahren auf Basis einschlägiger technischer Regeln und Normen beinhalten u.a. geeignete Ansätze für die Risikoanalyse und -bewertung und bieten einen deutlichen wirtschaftlichen und zeitlichen Vorteil für die Umsetzung und Akzeptanz. Das Technische Sicherheitsmanagement (TSM) ist bereits sektorenübergreifend (Gas, Wasser, Strom, Fernwärme, Abwasser) etabliert und behördlich anerkannt.

5. Das KRITIS-DachG und in Folge erlassene Rechtsverordnungen sollten für die Betreiber kritischer Infrastrukturen sowohl im nichtregulierten als auch im regulierten Bereich die notwendige rechtliche Sicherheit und Unterstützung bzw. Kostenanerkennung für Investitionen in die Resilienzerhöhung der physischen Sicherheit und der Abwehr von Bedrohungen sowie für Abhilfemaßnahmen zur Aufrechterhaltung des Betriebes im Falle eines erfolgreichen Angriffes geben.

   Dabei sollten auch Kosten anerkannt werden, welche über betriebliche Mittel und Maßnahmen für den Normalbetrieb hinausgehen. Solche Maßnahmen verhelfen zu mehr Versorgungssicherheit, wie etwa in Krisenfällen durch Naturkatastrophen, hybride Bedrohungen, Cyberangriffe oder terroristische Anschläge. Für Krisenfälle sieht der DVGW das KRITIS-DachG oder die noch folgenden Rechtsverordnungen als geeigneten Rahmen für die Festlegung von Mindestversorgungszielen für die Wasserversorgung, damit auch hier konkrete Maßnahmen und Investitionen getätigt werden können.

6. Der Referentenentwurf lässt zudem in weiten Teilen die Darstellung des Erfüllungs- und Umsetzungsaufwandes vermissen. Aufwände für die vorgeschriebenen Regulierungen werden die Kostensituation von Wirtschaftsunternehmen beeinflussen. Diese Annahme lässt

sich insbesondere durch den Bürokratieaufwand begründen. Zu erwartende Mehrkosten müssen daher anerkannt und umlagefähig auf die Produkte und Leistungen der jeweiligen Unternehmen sein. Für eine Abschätzung des Aufwandes sollte daher der Stand der Technik nicht erst im Nachgang festgelegt werden. Es ist weitgehend unbekannt, wie weit die zukünftigen Anforderungen gehen werden. Wie beim IT-Sicherheitsgesetz spricht sich der DVGW daher für die Festlegung eines Grundschutz zur physischen Sicherheit im KRITIS-DachG aus. Realistische Angaben zum Aufwand können erst dann gemacht werden, wenn der Stand der Technik festgelegt und damit der Aufwand definiert ist.

7. Gemäß den Vorgaben von § 78 Abs. 1 Nr. 1 iVm. § 79 Abs. 1 Nr. 1 TKG sind die Fernleitungsnetzbetreiber (FNB) dazu verpflichtet, Daten zu der von ihnen betriebenen Telekommunikationsstruktur der zentralen Informationsstelle des Bundes (ZIS) der Bundesnetzagentur (BNetzA) zu übermitteln. Diese Daten werden sodann im Infrastrukturatlas (ISA) veröffentlicht. Die Veröffentlichung dieser Daten stellt eine Gefahr für die Sicherheit der Gasversorgung in Europa und damit für die Kritische Infrastruktur dar. Die über den ISA veröffentlichte Telekommunikationsinfrastruktur verläuft parallel zu den von den FNB betriebenen Gasversorgungsleitungen und zeichnet damit ein genaues Lagebild des deutschen Erdgasversorgungssystems, einer der sensibelsten kritischen Infrastrukturen in Europa. Spätestens seit Februar 2022 hat sich die Sicherheitslage im Hinblick auf die Energie- und Telekommunikationsinfrastruktur in Deutschland und Europa deutlich verschlechtert. Zu nennen sind in diesem Zusammenhang z.B. die Sabotageakte Dritter auf die Erdgasleitungen Nord Stream 1 und 2 sowie auf die Eisenbahninfrastruktur in Deutschland. Wir halten es daher für geboten, die Veröffentlichung sensibler Infrastrukturdaten, die die kritische Infrastruktur Deutschlands unnötigen Gefahren aussetzt, zu vermeiden oder hiermit zumindest mit der Veröffentlichung entsprechender Daten sparsamer umzugehen, sofern an der Veröffentlichung dieser Daten kein überragendes öffentliches Interesse besteht. Eine entsprechende Regelung könnte dadurch erfolgen, dass die vorgenannten kritischen Infrastrukturen durch Verweis im KRITIS-DachG vom Veröffentlichungsgebot nach dem TKG ausgenommen würden.

## Positionen des DVGW im Einzelnen

Das zukünftige KRITIS-DachG sollte aus Sicht des DVGW die im Folgenden genannten zusätzlichen Anforderungen aufnehmen, damit die Belange der Gas- und Wasserversorgung angemessen Berücksichtigung finden und unter Rückgriff auf bestehende und bewährte technische und rechtliche Ordnungsrahmen beim Schutz von Kritischen Infrastrukturen sowie im Sinne des All-Gefahren-Ansatzes die Sicherheit und die Resilienz tatsächlich erhöht werden können.
Im Folgenden sind die Positionen zu den Regelungsinhalten der einzelnen Rechtsparagrafen erläutert:

## § 1 Zweck des Gesetzes

**Zusätzlich zu den formulierten Anforderungen ist die Aufnahme weiterer Anforderungen notwendig:**

- ausreichende finanzielle, materielle und personelle Unterstützung durch Bund und Länder bei Risiken, wie Sabotageakten durch terroristische Vereinigungen und Drittstaaten, welche zum Zeitpunkt der Risikoanalyse und -bewertung nach § 9 KRITIS-DachG nicht vorhersehbar sind und deshalb von den Betreibern kritischer Anlagen nicht berücksichtigt werden können.
- Absicherung für die Investition in physischen Schutz: Aufwendungen und Kosten zur Gefahrenabwehr der Betreiber müssen aufgrund der Zuständigkeit der Länder auch durch die Länder getragen werden. Hier dürfen die Grenzen des Bundesgesetzes nicht zulasten der Betreiber kritischer Anlagen gehen.
- Wahrung einer bundesweit einheitlichen Regelung zur Erhöhung der Resilienz: gerade für Versorgungsunternehmen, die in mehreren Bundesländern geschäftstätig sind, dürfen Öffnungsklauseln für die Länder nicht zu Anforderungsabweichungen auf Länderebene führen. Regelungen der Länder müssen sich an den Bundesregelungen orientieren und die bestehenden Regelungen beim Schutz Kritischer Infrastrukturen auch bezüglich der Kostenanerkennungen und Kostenerstattung berücksichtigen.

Schaffung einer gesetzlichen Grundlage für eine erweiterte Zuverlässigkeitsüberprüfung des Personals unterhalb der Sicherheitsüberprüfung (SÜV). Die Vertrauenswürdigkeit des Personals trägt in einem erheblichen Maße zur Resilienz kritischer Anlagen bei. Betreiber kritischer Anlagen sollten daher das Recht eingeräumt bekommen, eine erweiterte Zuverlässigkeitsüberprüfung des Personals unterhalb der Sicherheitsüberprüfungen im Umfeld kritischer Funktionen durchführen zu können. Unternehmen sollten bei Bedarf auf diesen Regelungsinhalt zurückgreifen können.

## § 2 Begriffsbestimmungen

**Harmonisierung der Begriffsbestimmungen:**

- Kritische Anlage (§ 2 Absatz 3 KRITIS-DachG): Die Konkretisierung des Begriffs ‚kritische Anlage' sollte auf bestehende Bestimmungen und Vorgaben (insbesondere BSI-KritisV) aufgesetzt werden, zudem sollte sie im KRITIS-DachG und NIS2UmsuCG einheitlich sein (aktuell abweichend zum Begriff im Referentenentwurf des NIS2UmsuCG). Im Sektor Energie muss die Konkretisierung des Begriffs in enger Abstimmung mit der BNetzA erfolgen.

  Grundsätzliche erscheint die Änderung des ursprünglichen Begriffs ‚kritische Einrichtung' (Art. 2 Nr. 1 und Nr. 4 CER) in ‚kritische Anlage' nicht zielführend. Der Grund mag in der Harmonisierung des KRITIS-DachG und der NIS-2-Richtlinie bzw. NISS2UmssuCG) liegen, allerdings ist die Nutzung der Begrifflichkeiten Anlage und Einrichtung und auch Infrastruktur innerhalb des KRITIS-DachG nicht konsistent.

- Die Begrifflichkeit ‚hybride Bedrohungen' sollte in § 2 Absatz 3 KRITIS-DachG definiert werden oder in § 9 KRITIS-DachG entsprechend aufgenommen werden. Der Begriff ist auf jeden Fall auslegungsbedürftig.

## § 3 Nationale zuständige Behörde für die Resilienz kritischer Anlagen

**Schaffung von bergreifenden institutionellen Strukturen der Krisenbewältigung und Koordinierung:**

- Angemessene Ausstattung des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe (BBK) mit personellen, finanziellen und technischen Ressourcen, damit das BBK seiner neuen Rolle als nationale zuständige Behörde für kritische Anlagen nachkommen kann
- In Fällen von Cyber- bzw. Informationssicherheitsvorfällen mit nationaler Tragweite enge Abstimmung des BBK mit der Bundesnetzagentur (BNetzA) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI): Um der behördlichen Zuständigkeit für die Resilienz kritischer Anlagen und die für diese nach dem All-Gefahren-Ansatz identifizierten Risiken insgesamt gerecht werden zu können.
- Erwägung der Einrichtung eines behördenübergreifenden nationalen Sicherheitslagezentrums sowie im Falle nationaler Krisenlagen und vor dem Hintergrund hybrider Bedrohungen die Einrichtung und Koordination eines nationalen Krisenstabs durch das BBK (§ 3 KRITIS-DachG)

Aus Sicht des DVGW wäre es perspektivisch wichtig, übergreifende institutionelle Strukturen der Krisenbewältigung und Koordinierung auszubauen und zu stärken. Krisenfälle in der jüngsten Vergangenheit wie das Hochwasser im Ahrtal haben gezeigt, dass dies dringend notwendig ist. Dazu bedarf es einer bundesweit einheitlichen Ertüchtigung bei Vorsorge und im Krisenmanagement, mit Standards für handlungs- und entscheidungsfähige kommunale und überörtliche Krisenstäbe, mit einer Rollenverteilung von kommunalen Strukturen und Hilfsorganisationen. Für die Katastrophenvorsorge sieht der DVGW dringenden Bedarf an verbindlichen und realitätsnahen begleiteten Trainingsformaten für Krisenstäbe, Organisationen unter Einbindung der Bevölkerung.

Ein wichtiger Baustein kann dabei der Aufbau und Betrieb einer bundesweiten zentralen Kompetenzplattform sein, die im Bedarfsfall in den dann betroffenen Regionen genutzt werden kann. Mit der Gründung des Gemeinsamen Kompetenzzentrums Bevölkerungsschutz (GeKoB) ist aus Sicht des DVGW der Anfang für den Aufbau einer solchen institutionellen Struktur gemacht, aber es Bedarf der weiteren Etablierung und Verzahnung mit dem KRITIS-DachG.

## § 4 Kritische Anlage

Eine umfängliche Kommentierung des Regelungsinhalts ‚kritische Anlage' im vorliegenden Entwurf des KRITIS-DachG (§ 2 (3) und §4) erfolgt nicht, da er der erst im Rahmen der zu erlassenden Rechtsverordnung abschließend geregelt werden soll (siehe dazu auch §§ 13 und 15 KRITIS-DachG).

## § 5 Verhältnis zu weiteren spezialgesetzlichen Regelungen

**Technische Regelsetzung als wesentliches Instrument zur Umsetzung des KRITIS-Dachgesetzes:**

- Um die Umsetzbarkeit und Wirtschaftlichkeit gesetzlicher Regelungsinhalte schon früh genug auch im Sinne der Rechts- sowie Planungssicherheit bewerten zu können, **sollten grundsätzlich wesentliche Regelungsinhalte wie Schwellenwerte und Anlagentypen, Einsatz kritischer Komponenten im KRITIS-DachG formuliert und nicht erst in der zu erlassenden Rechtsverordnung konkretisiert werden.** Der Zweck der zu erlassenden Rechtversordnung sollte darin bestehen, die Regelungsinhalte weiter auszugestalten. Dies ist Voraussetzung für eine realistische Schätzung der Erfüllungsaufwände der Wirtschaft.
- Anerkennung der Branchenspezifischen Sicherheitsstandards (Technisches Regelwerk) für den Sektor Wasser im Sinne der spezialgesetzlichen Regelungen nach § 5 KRITIS-DachG.
- Die Anerkennung der IT-Sicherheitskataloge der BNetzA im Sinne des § 5 KRITIS-DachG ist auch aus Sicht der Kostenanerkennung von Resilienzanforderungen durch die BNetzA sinnvoll und geboten. Ansonsten können im regulierten (Netz-)Geschäft anfallende Kosten aus Resilienzanforderungen nicht wirtschaftlich abgebildet werden.
- Weiterentwicklung der Branchenspezifischen Sicherheitsstandards, die im Geschäftsbereich des BSI liegen (z.B. B3S Wasser/Abwasser / W 1060), im Sinne der Resilienzerhöhung in Abstimmung mit dem BBK entsprechend der identifizierten Bedarfe bei der Resilienz

Im Sinne der Technischen Selbstverwaltung sollte für die Gas- und Wasserwirtschaft die Möglichkeit geschaffen werden, die Grundlage der IT-Sicherheitskataloge und Branchenspezifischen Sicherheitsstandards nach den identifizierten Bedarfen der Resilienzanforderungen entsprechend in den allgemein anerkannten Regeln der Technik als Branchenstandards (z. B. Technisches Regelwerk des DVGW) weiterzuentwickeln. Mit der CER ist ein länderübergreifender Ansatz gewählt. Insbesondere deshalb sollte die Weiterentwicklung im Zusammenspiel mit der einschlägigen internationalen und europäischen Normung (ISO 22300) erfolgen. Funktionale internationale/europäische Normen definieren den kleinsten gemeinsamen Nenner aller beteiligten Länder. Eine Revision bedarf der Mehrheitsentscheidung aller beteiligten Länder.

Nationale Sicherheitsstandards bieten - komplementär zu europäischen und internationalen Normen - eine effiziente und zeitlich flexiblere Möglichkeit angemessene Best Practice-Regelungen zu erstellen, anzuwenden und als deutschen Konsens in die Weiterentwicklung der internationalen und europäischen Normen einzubringen.

Insbesondere auf Seiten der Nachweisverfahren der Umsetzung von Sicherheit und Resilienz könnte dadurch auf bestehende Erfahrungen, Strukturen und bewährte Routinen für die Sektoren Energie und Wasser aufgebaut werden. Dadurch können neue Anforderungen schnell in bestehende Nachweisverfahren integriert werden. Dieser Ansatz für den Sektor Energie und Wasser ist auch deshalb sinnvoll, weil bereits bestehende Strukturen im Bereich Cybersicherheit und Sicherheitsmanagement (z. B. DVGW-TSM) zur Verfügung stehen und sich die Aufwendungen bei Wirtschaft und Verwaltung minimieren ließen.

## § 6 Anforderungen an Betreiber Kritischer Infrastrukturen

**Geeignetheit und Verhältnismäßigkeit technischer, sicherheitsbezogener und organisatorischer Maßnahmen zur Gewährleistung der Resilienz § 11 KRITIS-DachG:**

Mit dem Technischen Regelwerk des DVGW werden bereits heute besonders hohe Anforderungen an die Resilienz kritischer Infrastrukturen der Gas- und Wasserversorgung gestellt. Das Erreichen eines bestimmten Schwellenwertes ist hier keine Voraussetzung für die Pflicht zur Umsetzung der Anforderungen.

Die Branchenspezifischen Sicherheitsstandards (Technisches Regelwerk) sollten deshalb auch als weitere spezialgesetzliche Regelungen im Sinne des § 5 KRITIS-DachG anerkannt werden, weil sie schon heute schärfere Anforderungen an die Betreiber Kritischer Infrastrukturen im Sektor Gas- und Wasserversorgung stellen.

**Um die Umsetzbarkeit und Wirtschaftlichkeit gesetzlicher Regelungsinhalte schon früh genug auch im Sinne der Rechts- sowie Planungssicherheit bewerten zu können, sollten grundsätzlich wesentliche Regelungsinhalte nicht erst in der zu erlassenden Rechtsverordnung konkretisiert werden.**

**Daher wäre bereits im KRITIS-DachG ein Verweis auf die mindestens einzuhaltenden allgemein anerkannten Regeln der Technik über eine Vermutungsformulierung notwendig. Damit wäre bereits eine konkrete Ausgestaltung von Maßnahmen zur Resilienzerhöhung gegeben.**

Die Nutzung der Begrifflichkeiten Kritische Infrastruktur, kritische Anlage und kritische Einrichtung ist nicht konsistent und im Konflikt mit den Begrifflichkeiten in der CER-Richtlinie.

Aufgrund des inhaltlichen Umfangs der Begriffe kritische Infrastruktur und kritische Anlagen und die Verständlichkeit der Anforderungen wird empfohlen § 6 KRITIS-DachG vor § 4 KRITIS-DachG zu setzen.

## § 8 Registrierung der kritischen Anlage

**Es soll keine Doppelregistrierung von kritischen Anlagen erfolgen. Ist eine Anlage bereits über die etablierten Meldepflichten zum IT-Sicherheitsschutz oder über den physischen Schutz gemeldet worden, ist dies ausreichend.**

Der DVGW begrüßt ausdrücklich die geplante Transparenz, dass ‚kritische Anlagen zukünftig nur noch durch das KRITIS-DachG und die zugehörige Rechtverordnung bestimmt' werden (s. KRITIS-DachG, B Lösung) und die zugehörige Rechtsverordnung die Betreiberverpflichtungen im Hinblick auf physische Resilienzmaßnahmen nach dem KRITIS-DachG sowie im Hinblick auf die IT-Sicherheit nach dem BSIG transparent macht. Für die Registrierung und Meldung von erheblichen Störungen wird eine gemeinsame technische Lösung angestrebt.

Diese Rechtsvorgabe und die technischen Lösungen müssen eine einmalige Registrierung für **Betreiber für beide Rechtsbereiche vorsehen. Eine Doppelregistrierung ist in jedem Fall zu vermeiden!**

Bestehende Registrierungen nach § 8b Abs. 3 Satz 2 BSIG sollten für die Registrierungen nach § 8 KRITIS-DachG ohne erneute Registrierung anerkannt und in ein neues Register übernommen werden. Es soll keine Doppelregistrierung von kritischen Anlagen erfolgen. Ist eine Anlage einmal entweder über IT-Sicherheit oder Physischen Schutz gemeldet worden, muss dies ausreichen.

Die Liste registrierter Betreiber kritischer Anlagen sollte vertraulich (Vertraulichkeit, Geheimhaltung) behandelt werden und darf nicht veröffentlicht werden. Das BBK sollte entsprechende Schutzmaßnahmen ergreifen, um die Vertraulichkeit zu gewährleisten.

Deshalb sollte es nach § 16 KRITIS-DachG auch keine Ausnahmebescheide für das BBK und die beteiligten Behörden geben, die hinreichend hohen Vorgaben für die Vertraulichkeit im Wege stehen.

## § 9 Nationale Risikoanalysen und Risikobewertungen

**Bereitstellung kritischer Dienstleistungen (kDL) und nicht einer Versorgungssicherheit maßgeblicher Rahmen für Anforderungen an Betreiber kritischer Anlagen:**

Bestimmte durch die nationalen Risikoanalysen und -bewertungen nach § 9 KRITIS-DachG identifizierte Risiken (z. B. Sabotageakte, die durch terroristische Vereinigungen oder durch Drittstaaten verübt werden) können durch die Betreiber kritischer Anlagen in ihren Resilienzplänen nur bedingt berücksichtigt werden. In diesen Fällen sollten Bund und Länder auch im Sinne der EU-Richtlinien zum Schutz Kritischer Infrastrukturen (CER-Richtlinie) die Betreiber kritischer Anlagen angemessen finanziell und personell unterstützen.

Die Begrifflichkeit ‚hybride Bedrohungen' sollte in § 2 KRITIS-DachG definiert werden oder in § 9 KRITS-DachG aufgenommen werden. Der Begriff ist auf jeden Fall auslegungsbedürftig.

Der DVGW bietet gerne bereits zur Erstellung der Nationalen Risikoanalysen und Risikobewertungen seine Unterstützung an und bittet um eine enge Einbindung bei deren Erstellung. Nach den Erfahrungen der branchenspezifischen Risikoanalysen im Vorfeld des IT-Sicherheitsgesetzes hat sich diese Vorgehensweise bewährt. Damit ließen sich die Erfahrungen der Branchen berücksichtigen, um realitätsnahe Risiken zu benennen und entsprechende Anforderungen festzulegen.

## § 10 Risikoanalysen und Risikobewertungen der Betreiber kritischer Anlagen in Verbindung mit § 9 Nationale Risikoanalysen und Risikobewertungen

**Möglichkeit der Anerkennung von bestehenden und als gleichwertig angesehenen Risikoanalysen und -bewertungen nach § 10 KRITIS-DachG sowie von Nachweisen und Zertifikaten aus bestehenden Sicherheitsmanagementsystemen in Abstimmung zwischen BBK mit BNetzA oder BSI nach § 11 KRITIS-DachG:**

- Anerkennung bestehender Sicherheits-, Risikomanagementsysteme zur Risikoanalyse und Risikobewertungen und Sicherheitsstandards der Betreiber kritischer Anlagen mit ganzheitlichem übergreifenden Bezug zu anderen Gesetzen und Verordnungen wie u.a. EnWG, TrinkwV, TrinkwEzgV

  Die bestehenden branchenspezifischen Risikomanagementsysteme zur Risikoanalyse und Risikobewertungen sowie Sicherheitsstandards und IT-Sicherheitskataloge der BNetzA sollten für den Sektor Energie und Wasser im Sinne der weiteren spezialgesetzlichen Regelungen nach § 5 KRITIS-DachG als Grundlage für Risikoanalysen und Risikobewertungen nach §§ 9, 10 KRITIS-DachG anerkannt werden. Im Sinne der Technischen Selbstverwaltung sollte das KRITIS-DachG für die Gas- und Wasserwirtschaft die Möglichkeit schaffen, die IT-Sicherheitskataloge der BNetzA und die branchenspezifischen Sicherheitsstandards nach den

identifizierten Bedarfen der Risikoanalysen und -bewertungen, entsprechend § 11 Absatz 5 weiterzuentwickeln.

- Anerkennung von bestehenden Nachweisen und Zertifikaten in Abstimmung von BBK mit BNetzA, UBA oder BSI nach § 11 KRITIS-DachG

  Nachweise zur Einhaltung bereits etablierter Risiko- und Sicherheitsmanagementsysteme (z. B. Technisches Sicherheitsmanagement des DVGW TSM) der mindestens einzuhaltenden anerkannten Regeln der Technik sollten nach § 11 KRITIS-DachG anerkannt werden, um keinen zusätzlichen Aufwand zu erzeugen. Es sollten bereits bestehende Systeme, Strukturen und Dienstleistungen im Bereich der Nachweisführung (Zertifizierung) genutzt und ggf. ausgebaut werden.

- Anerkennung von branchenspezifischen Sicherheitsstandards nach § 5 KRITIS-DachG.

- Bewertung geopolitischer Abhängigkeiten von Drittländern können nur durch oder mit Unterstützung von Behörden erfolgen.

  Die Bewertung der Abhängigkeiten insbesondere nach geopolitischen Maßgaben von Drittländern kann nicht durch die Risikoanalyse und -bewertung der Betreiber kritischer Anlagen erfolgen. Über die dafür notwendigen Informationskanäle und Kompetenzen verfügen nur das Auswärtige Amt sowie die geheimdienstlichen Behörden. Deshalb sollte die Risikoanalyse und -bewertung bezüglich der Abhängigkeit von Drittländern auch ausschließlich Aufgabe der nationalen Risikoanalyse und -bewertung nach § 9 KRITIS-DachG sein.

- Betreiber kritischer Anlagen werden verpflichtet erstmals 9 Monaten nach der Registrierung (§ 8 KRITIS-DachG) und dann spätestens alle 4 Jahre Risikoanalysen und -bewertungen vorzulegen. Diese basieren auf den Vorgaben aus den Nationalen Risikoanalysen und -bewertungen nach § 9 KRITIS-DachG, die alle vier Jahre vom sektorenzuständigen Bundesministerium erstellt, vom BBK auswertet und den Betreibern kritischer Anlagen zur Verfügung gestellt werden.

  Das KRITIS-DachG sollte diese Zeitvorgabe im Sinne der Betreiber konkretisieren, z. B. durch die Aufnahme der behördlichen Verantwortung für eine eindeutige Firstvorgabe unter Berücksichtigung der tatsächlichen Zustellung der Risikoanalyse und -bewertungen aus § 10 (1) KRITIS-DachG an den Betreiber kritischer Anlagen. Es sollte klargestellt werden, auf welcher Basis Betreiber kritischer Infrastrukturen Risikoanalysen und Risikobewertungen entsprechend § 10 KRITIS-DachG erstellen, wenn Nationale Risikoanalysen und Risikobewertungen gemäß § 9 KRITIS-DachG nicht rechtzeitig vorliegen.

  Weiterhin muss vorgeben werden, welche Fristen für bereits registrierte Anlagen gelten.

## § 11 Resilienzmaßnahmen der Betreiber kritischer Anlagen

**Möglichkeit der Erstellung von Branchenspezifischen Resilienzstandards durch Branche und ihre Branchenverbände nach § 11 KRITIS-DachG:**

- Anerkennung von Branchenspezifischen Sicherheitsstandards nach § 5 KRITIS-DachG der Technischen Regelsetzung als wesentliches Instrument zur Umsetzung des KRITIS-Dachgesetzes durch Aufnahme einer Vermutungsregelung in Analogie zum § 49 EnWG und der Trinkwasserverordnung, dass mindestens die allgemein anerkannten Regeln der Technik einzuhalten sind. Mit einer solchen Formulierung wäre ebenso die Einhaltung des Standes der Technik abgedeckt.

Die Ausgestaltung der Branchenspezifischen Sicherheitsstandards im Detail sollte über die seit Jahrzehnten bewährte Technische Regelsetzung in der Gas- und Wasserversorgung erfolgen. Der Verweis auf allgemein anerkannte Regeln der Technik und die entsprechende Ausgestaltung und Schaffung von Standards durch die Technische Regelsetzung haben sich in der Abwasserentsorgung und Trinkwasserversorgung sowie in der Gas- und Stromversorgung bewährt. Dies sollte in dem KRITIS-Dachgesetz in einer Formulierung analog dem § 49 Energiewirtschaftsgesetz ermöglicht werden.

Die Technischen Regeln des DVGW machen heute schon weiterführende Vorgaben zur Resilienz der Infrastruktur (DVGW W 1050 oder DVGW W 1003) sowie zum Risiko- und Krisenmanagement in der Gas-, Wasserstoff- und Trinkwasserversorgung (DVGW G 1001, G 1002, G 1003, W 1001). Solche Technischen Regeln und deren Weiterentwicklung innerhalb der jeweiligen Branchen sollten daher ein wesentlicher Bestandteil für die Umsetzung des KRITIS-Dachgesetzes sein, um eine effektive Umsetzung der gesetzlichen Regelungen und eine Verbesserung der Sicherheitslage in der Praxis zu ermöglichen.

Durch die Technische Regelsetzung (z. B. DVGW) gemäß Vermutungsregelung nach § 49 EnWG und der Trinkwasserverordnung sollte der Gas- und Wasserwirtschaft die Möglichkeit geschaffen werden, die Normengrundlage der IT-Sicherheitskataloge und Branchenspezifischen Sicherheitsstandards nach den identifizierten Bedarfen bei Resilienzmaßnahmen entsprechend weiterzuentwickeln. Daher sollte auch hier, um die Umsetzbarkeit und Wirtschaftlichkeit gesetzlicher Regelungsinhalte schon früh genug auch im Sinne der Rechts- sowie Planungssicherheit bewerten zu können, Regelungsinhalte konkretisiert werden. Daher wäre bereits im KRITIS-DachG und/oder in den in Folge erlassenen, sektorenspezifischen Verordnungen nach § 15 KRITIS-DachG ein Verweis auf die mindestens einzuhaltenden allgemein anerkannten Regeln der Technik über eine Vermutungsformulierung sinnvoll. Damit wäre bereits eine konkrete Ausgestaltung von Maßnahmen zur Resilienzerhöhung gegeben.
Im Sinne der Resilienzerhöhung ließe sich die Fortschreibung von Branchenspezifischen Standards damit in bereits bestehenden und etablierten Strukturen der Technischen Regelsetzung und Normung unter Beteiligung von Institutionen, Behörden und der jeweiligen Branchen umsetzen, ohne neue Strukturen aufbauen zu müssen.

- Bez. der Eignungsfeststellung der Branchenspezifischen Sicherheitsstandards (§ 11 (5) KRITIS-DachG, erfolgt keine Festlegung des konkreten Prozesses. Mit Blick auf die Harmonisierung mit dem den Vorgaben zur IT-Sicherheit sollte die Frist zur Anerkennung branchenspezifischer Standards für die Weiterentwicklung erhöht werden. Derzeit ist eine erneute Anerkennung nach dem BSIG alle 2 Jahre erforderlich. Aus den Erfahrungen mit der Fortschreibung des B3S würde eine Fristverlängerung, die Qualität der operativen Umsetzung durch die KRITIS-Betreiber deutlich erhöhen. Eine Anpassung der Zeitschiene für branchenspezifische Sicherheitsstandards für IT-Sicherheit ist ebenso in Erwägung zu ziehen.

- Aus § 11 (13) KRITIS-DachG ergibt sich die Verpflichtung frühestens 10 Monate nach Registrierung Resilienzmaßnahmen zu ergreifen, die auf den Risikoanalyse und -bewertungen basiert. Mit Blick auf die Umsetzbarkeit für die Betreiber kritischer Anlagen sollte der Begriff ‚frühestens' konkretisiert werden. Ggf. sollte das KRITIS-DachG eine Übergangsregelung oder einen Rückgriff auf das bewährte System der anerkannten Regeln der Technik vorsehen.

Im Sinne der Hebung von Synergien und Effizienzen sollten bestehende Dokumente, Zertifikate und Maßnahmen aus der Cyber-, Informationssicherheit und technischen Sicherheit so weit wie möglich

anerkannt werden. Schon heute werden über Sicherheitsmanagementsysteme (z. B. Technisches Sicherheitsmanagement TSM des DVGW), die dafür auf etablierte und bewährte allgemein anerkannte Regeln der Technik (z. B. DVGW-Regelwerk) zurückgreifen, Resilienz-Risiken im Sinne des All-Gefahren-Ansatzes erfasst und geeignete Maßnahmen zu ihrer Mitigierung beschrieben sowie umgesetzt. Im Sinne des Ziels, die Resilienz kritischer Infrastrukturen zu erhöhen, sollte bei der Entwicklung von Branchenspezifischen Resilienzstandards auf den bestehenden und bewährten Technischen Regeln aufgebaut werden.

Nachweise zur Einhaltung der Resilienzmaßnahmen nach den mindestens einzuhaltenden anerkannten Regeln der Technik sollten nach § 11 KRITIS-DachG anerkannt werden, um nicht einen zusätzlichen Aufwand zu erzeugen und auf bereits bestehenden Systemen aufzubauen sowie vorhandene Strukturen und Dienstleistungen im Bereich der Nachweisführung (z. B. durch Zertifizierung) zu nutzen.

## § 12 Meldewesen für Störungen

**Zentrales Melde- und Informationsportal nach § 12 KRITIS-DachG:**

- Die Umsetzung eines zentralen Melde- und Informationsportals sollte am Stand der Technik für Portale und ihrer Absicherung erfolgen. Grundlage für die Meldungen im Sinne eines ganzheitlichen Ansatzes könnte z.B. das BSI-Meldeformular sein, das um einen Abschnitt zu physischen Vorfällen ergänzt werden könnte. § 12 Absatz 2 Kritis DachG fordert für Meldungen die Übermittlung sämtlicher verfügbarer Informationen damit die Art, Ursache und mögliche Folgen eines Vorfalls nachvollzogen und ermittelt werden können. Hier ist eine Präzisierung im Hinblick auf sämtlich verfügbare Informationen wünschenswert, um eventuelle Nachfragen seitens der Behörden im Kommunikationsprozess mit dem Betreiber zu vermeiden bzw. zu minimieren. Hier wäre ein Kriterienkatalog hilfreich, was an physischen Vorfällen gemeldet werden muss. Mehrfachmeldung/Doppelmeldungen (BNetzA, BSI und zukünftig BBK) sollten vermieden werden. Daher sollte unbeschadet anderer gesetzlicher Meldeverpflichtungen nur eine Meldepflicht z. B. für IT-Sicherheitsvorfälle nur gegenüber dem BSI bestehen.

  Der DVGW begrüßt ein zentrales Melde- und Informationsportal ausdrücklich. Ein zentrales, gemeinsames Portal vermeidet gerade im Zusammenhang mit ausführlichen Berichten die Überlastung des Meldeprozesses. Grundlage für die Meldungen im Sinne eines ganzheitlichen Ansatzes könnte z. B. das BSI-Meldeformular sein, das um einen Abschnitt zu physischen Vorfällen ergänzt werden könnte. Für die Betreiber wäre es hilfreich, wenn das BBK im Einvernehmen mit dem BSI keine neue Meldestelle festlegen würde, sondern die bereits vorhandenen Kommunikationskanäle bestätigt.
- Alle verfügbaren Informationen zu einem Vorfall können nicht bereitgestellt werden. Die Betreiber kritischer Anlagen können aber alle für den Vorfall relevanten Daten bereitstellen.
- Nachgelagerte Behördenprozesse sollten reibungslos aufgesetzt sein.

## § 13 Einsatz kritischer Komponenten - Verordnungsermächtigung

**Wahrung der Verhältnismäßigkeit für die Beschaffung und den Einsatz kritischer Komponenten:**

- Keine Übertragung des Verfahrens nach § 9b BSIG i.V.m. § 11 Abs. 1g EnWG auf kritische Komponenten im Sinne des § 13 KRITIS-DachG.

  Das bisherige Verfahren des § 9b BSIG hat sich weder im Telekommunikationssektor noch im Sektor Energie als geeignetes Mittel bewährt, um die technologische Abhängigkeit bei Schlüsseltechnologien bzw. kritischen IT-Komponenten spürbar und nachhaltig zu verringen.

Der DVGW fürchtet daher, dass Beschaffungsvorbehalte bei kritischen Komponenten den Beschaffungsprozess unverhältnismäßig erschweren. Es besteht auch die Gefahr, dass die Festlegungen in das EU-Ausschreibungsrecht zu Lasten der betroffenen Unternehmen eingreift und ggf. zu Marktverzerrungen wegen Ungleichbehandlung führen.

Die Kriterien zur Auswahl von einsetzbaren „kritischen Komponenten“ müssen zwingend mit den Betreibern bzw. Branchenverbänden festgelegt und kommuniziert werden. Die Beschaffung der Komponenten und die notwendige kurzfristige Reaktionsfähigkeit zur Aufrechterhaltung der Sicherheit – im Gefahrenfall – muss jederzeit möglich sein. Eine Untersagung des Einsatzes von bereits eingesetzten Komponenten zum Zeitpunkt des Inkrafttretens des Gesetzes muss verhältnismäßig und unter Wahrung einer ausreichenden Übergangsfrist erfolgen (Bestandsschutz). Die angedachte Neuregelung birgt ansonsten die Gefahr, die Sicherheit in kritischen Infrastrukturen zu schwächen. Die Beschaffbarkeit kritischer Komponenten ist essenziell für die Versorgungssicherheit – bei vorliegenden Versorgungsengpässen für kritische Komponenten, sollte eine Güterabwägung zwischen Konformität der Vorgaben für kritische Komponenten und der Versorgungssicherheit im Sinne der Beschaffung erfolgen.

## § 14 Berichtspflichten

**Verhältnismäßigkeit bei Transparenzpflichten für KRITIS-Betreiber:**

- Umfassende Berichtspflicht gegenüber Kommission birgt ein nicht unerhebliches Bündelungsrisiko bezüglich sensitiver Daten.

  Der Nutzen umfassender Berichtspflichten an die Kommission ist vor dem Hintergrund der Fülle von Berichten aus allen Unionsmitgliedstaaten fraglich. Vielmehr besteht sogar ein nicht unerhebliches Bündelungsrisiko, da eine Fülle sehr sensitiver Daten zur Resilienz kritischer Anlagen an eine Institution übergeben werden soll. Gegenwärtig ist auch kein Feedback-Prozess Richtung Betreiber kritischer Anlagen angedacht, der einen echten Mehrwert etwa in Bezug auf Entwicklungen von europäischer Relevanz für die Betreiber kritischer Anlagen bieten könnte.
- Betreiber kritischer Anlagen müssen beim Vorliegen von Entwicklungen oder Vorfällen von europäischer Relevanz Zugang zu relevanten Informationen aus dem Berichtswesen an die Kommission erhalten.
- Verhältnismäßigkeit bei Transparenzpflichten für Betreiber kritischer Anlagen
- geeigneten effizienten Informationsaustausch zwischen den für Betreibern kritischer Anlagen zuständigen Behörden, mit Nachrichtendiensten und auch den Betreibern kritischer Infrastrukturen

Gegenwärtig unterliegen Betreiber kritischer Infrastrukturen sowohl auf Ebene des Bundes als auch auf Ebene der Länder einer Vielzahl von Informationsfreiheits- und Transparenzgesetzen (auf Bundesebene z. B. das IFG, das GeoZG und das UIG). Darüber hinaus bestehen aber auch speziellere Normen, die eine Datenherausgabe anordnen. Dies schließt etwa Informationen zur Art, zur gegenwärtigen Nutzung, zur tatsächlichen Verfügbarkeit und zur geografischen Lage des Standortes und der Leitungswege dieser Einrichtungen ein.
Für kritische Infrastrukturen bestehen jedoch in einigen Fällen Ausnahmen, was die Herausgabe bestimmter sensibler Daten betrifft. Allerdings müssen teilweise auch in diesen Ausnahmefällen die Informationen erst an eine zentrale Informationsstelle gesendet werden, um dann eine Ausnahmeantrag stellen zu können, damit diese Informationen nicht veröffentlicht werden (vgl. §§ 79 Abs. 2 S. 1/Abs. 3 Nr. 3 TKG).

Insgesamt sollte sichergestellt werden, dass Informationen über die kritischen Infrastrukturen nicht zu einfach über die Informationsfreiheits- und Transparenzgesetze zugänglich sind. Im Rahmen des KRITIS-DachG sollten Betreiber kritischer Anlagen von den tiefgreifenden gesetzlichen Transparenzpflichten ggf. ohne Stellung eines Antrags ausgenommen werden.

Es handelt es sich beispielsweise um Informationen zu

- § 9 – Nationale Risikoanalyse und Risikobewertung
- § 10 – Risikoanalysen und Risikobewertungen der Betreiber kritischer Anlagen
- § 11 – Maßnahmen zur Resilienz und Dokumentation dazu insbesondere Sicherheits- und Resilienz-Konzepte
- § 12 – Meldungen zu Störungen
- § 14 – Meldungen des BBK an die Europäische Kommission

Im Gesetz sollten daher entsprechende Regelungen zum Geheimschutz verankert werden. Wir schlagen daher vor, diese Informationen, entsprechend Geheimschutz, als VS vertraulich zu klassifizieren.

Informationen über kritische Infrastrukturen sollten zudem nicht wie im Fall des § 79 Abs. 3 Nr. 3 TKG an einem zentralen Punkt gesammelt und gespeichert werden, bevor über ihre Veröffentlichung konkret entschieden wird. Würde diese Praxis im Rahmen des KRITIS-Dachgesetzes angewendet, so würden dadurch an einem einzigen Punkt viele sensible Informationen zusammenlaufen und ein „single point of failure“ geschaffen. Wird diese zentrale Informationsstelle kompromittiert, besteht Zugriff auf eine Vielzahl von Informationen über kritische Infrastrukturen von einer Vielzahl von Betreibern.

In verschiedenen Situationen fragen Behörden (z. B. Bundesbehörden oder Landeskriminalämter) bei Branchenexperten Informationen ab; allerdings verhindern z. B. Geheimhaltungspflichten und Quellenschutz das Teilen und den Austausch notwendiger Informationen zwischen den unterschiedlichen Behörden, mit Nachrichtendiensten und/oder mit den Fachexperten.
Das KRITIS-DachG sollte die Grundlage für einen geeigneten effizienten Informationsaustausch zwischen den für KRITIS zuständigen Behörden, mit Nachrichtendiensten und auch den Betreibern kritischer Infrastrukturen schaffen. Es sollte zudem vorsehen, dass die Informationen aus den Branchen zeitnah, abstrakt und anonymisiert den Branchen als Rückinformation wieder zur Verfügung gestellt werden, um einen beidseitigen Nutzen zu schaffen. Es würde z. B. dabei helfen,

Sicherheitslücken, die bei einem Betreiber von kritischen Infrastrukturen aufgefallen sind, auch bei anderen Betreibern proaktiv zu schließen.

## § 15 Ermächtigung zum Erlass von Rechtsverordnung

**Schärfung und Konkretisierung von KRITIS-DachG in der zu erlassenden Rechtsverordnung erforderlich:**

Das KRITIS-DachG muss in der zu erlassenden Rechtsverordnung geschärft und konkretisiert werden, damit das KRITIS-DachG sowie die zu erlassende Rechtsverordnung im Sinne des All-Gefahren-Ansatzes die größte Wirksamkeit entfalten und maximale Synergien heben kann. Die zu erlassende Rechtsverordnung sollte daher der weiteren sektorspezifischen Detaillierung der Anforderungen dienen und auf den Sektorstudien des BSI und der daraus abgeleiteten BSI-KritisV aufbauen und die dort erarbeiteten Methoden zur Bestimmung von Schwellenwerten und Anlagenkategorien übernehmen.

**Eine frühzeitige und umfassende Einbindung der Branchen und ihrer Verbände wäre aus Sicht des DVGW sinnvoll und wünschenswert. In der Erarbeitung und Umsetzung der BSI-KritisV war dies ein anerkannt erfolgreicher Ansatz.**

## § 16 Ausnahmebescheid

**Grundsätzlich keine Ausnahmen:**

- Es sollte keine Ausnahmen für Behörden geben, die zu einem abweichenden und im Vergleich zur Wirtschaft niedrigeren Schutzniveau bei der Resilienz und der Informations-sicherheit (siehe auch § 12 KRITIS-DachG insbesondere zentrales Melde- und Informationsportal) führen.
- Ausnahmen sollten nicht für die Dienstleister der Verwaltung gelten.

Ausnahmen sollten nicht für die Dienstleister der Verwaltung gelten. Es sollte ferner grundsätzlich keine Ausnahmen für Behörden geben, die zu einem abweichenden und im Vergleich zur Wirtschaft niedrigeren Schutzniveau bei der Resilienz führen. Insbesondere (kommunale) Verwaltungen haben sich in den letzten Jahren dem Angriffsgeschehen aus dem Cyberraum teilweise als nicht gewachsen gezeigt. Sie stellten damit im Cyber- und Informationsraum das „Einfallstor“ für die Verbreitung von Angriffen auf (kommunale) Unternehmen der Daseinsvorsorge dar. Diesem Risiko muss auch bei der Resilienz durch vergleichbare Sicherheits- bzw. Resilienzniveaus begegnet werden.

## § 17 Verarbeitung personenbezogener Daten

**Keine Notwendigkeit zur Erhebung personenbezogener Daten:**

Der DVGW ist der Auffassung, dass für die Erstellung von Risikoanalysen und -bewertungen bzw. für die Ableitung von Resilienzmaßnahmen keine personenbezogenen Daten benötigt werden.

## Anhang 1

**Unterstützung durch Branchenverbände:**

Der DVGW wird das BBK bei der weiteren Ausgestaltung der Anforderungen und Maßnahmen sowie der Erstellung der Vorlagen und Muster zur Unterstützung der Betreiber kritischer Anlagen der Gas- und Wasserversorgung unterstützen.