

Berlin, 24. Januar 2024

---

## **Deutsche Industrie- und Handelskammer**

---

Referentenentwurf des Bundesministeriums des Innern und für Heimat

### **Entwurf eines Gesetzes zur Umsetzung der CER-Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz von Betreibern kritischer Anlagen (KRITIS-Dachgesetz und weitere)**

Wir bedanken uns für die Gelegenheit zur Stellungnahme zu dem o. g. Entwurf.

Staat und Wirtschaft sind gemeinsam gefordert, die Sicherheit der Netze und kritischer Anlagen zu gewährleisten. Einheitliche Maßstäbe zur Verbesserung der Sicherheit, insbesondere kritischer Infrastrukturen, sind von besonderer Bedeutung für das Funktionieren der gesamten deutschen Wirtschaft. Das Gesetz adressiert dieses Anliegen, indem es die physische Sicherheit und Resilienz von Betreibern kritischer Infrastrukturen stärken soll. Es setzt die EU CER-Richtlinie (EU 2022/2557) um und reguliert Betreiber kritischer Anlagen mit zusätzlichen Maßnahmen und Pflichten insbesondere in den Bereichen Business Continuity Management, physische Sicherheit, Risiko- und Krisenmanagement.

### **Das Wichtigste in Kürze**

Die Sicherheit der kritischen Infrastrukturen gewinnt immer mehr an Bedeutung. Insbesondere der russische Angriffskrieg gegen die Ukraine, aber auch zunehmende geopolitischen Spannungen, haben sicherheitsrelevante Auswirkungen auf Infrastrukturen und Lieferketten. Sind diese ganz oder teilweise nicht verfügbar, drohen Schäden für die gesamte Wirtschaft. Wir stimmen ausdrücklich dem Ziel des Gesetzes zu, die physische Resilienz von Betreibern kritischer Anlagen zu verbessern. Bei der Erhöhung der Resilienz lassen sich physische Sicherheit und die Sicherheit von Daten und Informationen nicht mehr trennen. Sie sollten im Zusammenhang betrachtet werden. Mit dem NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) werden die Regelungen zum Cyberschutz von Kritischen Infrastrukturen und weiteren wichtigen Einrichtungen weiterentwickelt. Das sog. KRITIS-Dachgesetz soll neben diese Regelungen treten und den physischen Schutz kritischer Anlagen regeln.

Die Unternehmen benötigen klare rechtliche Vorgaben, um rechtssicher handeln zu können. Das BMI hat viele Kritikpunkte unserer [Stellungnahme](#) zum Entwurf eines Kritis-Dachgesetzes vom August 2023 im nun vorliegenden Referentenentwurf aufgegriffen. Dies trägt zur Verständlichkeit und einer besseren Systematik der Regelungen bei. Unternehmen befürchten jedoch weiterhin Doppelregulierungen und Inkonsistenzen, die einer effektiven und effizienten Umsetzung entgegenstehen. Wünschenswert wäre gewesen, zumindest die beiden oben genannten Referentenentwürfe aufgrund der inhaltlichen Zusammenhänge parallel zur Diskussion zu stellen.

Aus Sicht von Unternehmen müssen die Regelungen des Kritis-Dachgesetzes praktisch und mit angemessenem Aufwand umsetzbar sein und vor allem dem Ziel der eigenen Unternehmenssicherheit dienen. Das Gesetz sollte dafür Mindestanforderungen definieren. Die dazu nötige Diskussion muss mit der Wirtschaft geführt werden. Zusätzlich sollte die Umsetzung durch unterstützende Maßnahmen und effektive Zusammenarbeitsprozesse zwischen Staat und Wirtschaft flankiert werden.

Insbesondere vor dem Hintergrund, dass zusätzlich zum Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) weitere Aufsichtsbehörden von Bund und Ländern für die Umsetzung verantwortlich zeichnen, die sich untereinander vernetzen müssen, sollten die Prozesse der Zusammenarbeit zwischen den Behörden klar definiert werden. Nur so lassen sich Doppelaufwand für die Unternehmen, z. B. durch Mehrfachmeldungen, verhindern und umgekehrt effektive Warnhinweise an die Unternehmen gewährleisten. Alle Maßnahmen müssen darauf hinwirken, das Schutzniveau der Unternehmen zu verbessern und deren eigene Sicherheitsbemühungen zu unterstützen. Die öffentliche Hand sollte den Unternehmen insbesondere passgenaue Informationen zur aktuellen Sicherheitslage (Cyber- und analoge Bedrohungen) mit konkreten Handlungsempfehlungen zur Verfügung stellen. Eine angemessene personelle Ausstattung der Behörden ist Voraussetzung dafür.

Erforderlich wäre ein übergreifendes Gesamtkonzept, das analoge und digitale Sicherheit von Staat, Wirtschaft und Gesellschaft umfassend und gleichermaßen adressiert und in Bezug auf die Belastungen der betroffenen Unternehmen dem Angemessenheitsprinzip Rechnung trägt. Eine aus einem solchen Gesamtkonzept abgeleitete KRITIS-Resilienzstrategie – die eigentlich Grundlage dieses Gesetzes sein müsste – soll jedoch erst bis zum 17. Januar 2026 durch die Bundesregierung verabschiedet werden. Die im Entwurf skizzierte Chronologie der Umsetzungserfordernisse ist eine Herausforderung, die leicht aus dem Takt kommen kann – insbesondere durch die nötigen Abstimmungen zwischen BBK, BSI sowie weiteren Behörden auf Bundesebene und auf Ebene der Bundesländer. Unternehmen dürfen keine Nachteile oder Zusatzaufwände entstehen, wenn sich der Zeitplan ändert.

## **Im Einzelnen**

### **Begriffsbestimmungen (§ 2)**

Hier wurde nachgebessert, indem parallele Definitionen entfernt und Sektoren in Bezug auf die NIS2-Umsetzung entfernt wurden.

### **Betroffenheit von Unternehmen (§§ 4, 6, 16)**

Betreiber müssen ihre kritischen Anlagen selbst identifizieren. Eine Anlage gilt grundsätzlich dann als kritisch, wenn sie zum Stichtag den Sektoren Energie, Transport und Verkehr, Finanz- und Versicherungswesen, Gesundheitswesen, Trinkwasser, Abwasser, Ernährung, Informationstechnik und Telekommunikation, Weltraum oder Siedlungsabfallentsorgung zuzuordnen ist und bestimmte Schwellenwerte erreicht oder überschreitet. Dabei gilt grundsätzlich der Regelschwellenwert von 500.000 zu versorgenden Einwohnern. Hier sind Flexibilisierungen vorgesehen. Auch kleinere Einrichtungen unterhalb des Regelschwellenschwertes sollen unter bestimmten Bedingungen unter das KRITIS-Dachgesetz fallen können. Die Anlagenarten, Schwellenwerte etc. sollen durch eine Verordnung konkretisiert werden, die noch nicht vorliegt. Die Rechtsverordnung soll für das Kritis-Dachgesetz und das NIS2UmsuCG gleichermaßen gelten.

Die Unternehmen benötigen frühzeitig Rechtssicherheit und es muss einfach zu beurteilen sein, ob sie vom Kritis-Dachgesetz und/oder NIS2UmsuCG betroffen sind, und welche Pflichten sich für sie ergeben. Bei den entsprechenden Begrifflichkeiten und Definitionen sollte entsprechend nachgebessert werden. Wesentliche Inhalte, die über die Betroffenheit bestimmen, werden in nachrangige Rechtsakte mit geringeren Beteiligungsmöglichkeiten für die Wirtschaftsverbände verlagert. Hier ist lediglich eine Anhörung vorgesehen. Die konkretisierenden Rechtsverordnungen sollten zeitnah verabschiedet werden und dann tatsächlich für beide o. g. Gesetze gelten. Grundsätzlich weisen wir an dieser Stelle darauf hin, dass sich die Kommentierung des Gesetzentwurfs aufgrund der fehlenden Rechtsverordnung insgesamt als schwierig gestaltet, weil so für die Unternehmen ihre tatsächliche Betroffenheit schwer abschätzbar ist. Wir gehen außerdem davon aus, dass die Vorgaben auch Auswirkungen entlang der Lieferkette haben werden, die aktuell nicht abschätzbar sind.

Positiv ist, dass die Systematik zur Bestimmung von KRITIS grundsätzlich beibehalten werden soll (§ 4 Abs 1). Zwar wurde im Kritis-Dachgesetz der Schwellenwert von 500.000 zu versorgenden Einwohnern gesetzt. Diese Systematik wird jedoch „aufgebrochen“, wenn Behörden nach entsprechendem Ermessen zukünftig einseitig die Identifizierung als Betreiber kritischer Anlagen vornehmen können (§ 4 Abs 2). Hierfür maßgebliche Kriterien sind zwar im Entwurf aufgeführt, werden jedoch teilweise nicht näher eingegrenzt, zum Beispiel „Auswirkungen auf wirtschaftliche und gesellschaftliche Tätigkeiten“ (Nummer 3) oder der „Marktanteil des Betreibers“ (Nummer 4). Hier bräuchte es nachvollziehbare und angemessene Kriterien.

Auch weitere begriffliche Ungenauigkeiten sollten bereinigt werden. Während die CER- und die NIS2-Richtlinie sich auf den Begriff „Einrichtungen“ fokussieren, stellt das KRITIS-Dachgesetz auf „Anlagen“ ab (zum Beispiel in § 4 Abs 1). Darüber hinaus können nach § 4 Abs 2 „weitere Betreiber“ festgelegt werden. Unklarheiten bestehen auch bei den Begriffsbestimmungen in § 4 und § 16. Es sollten einheitlich Betreiber kritischer Anlagen adressiert werden, und dies gesetzesübergreifend konsistent.

Die in § 4 enthaltene Sektorenbezeichnung erscheint unvollständig oder unpräzise, z. B. ist das "Bankwesen" nicht enthalten, obwohl in § 4 Abs 6 eine Rückausnahme enthalten ist. Der "Digitalsektor" wird in der Gesetzesbegründung häufiger erwähnt, obwohl er in § 4 Abs 1 nicht genannt wird.

Die Sektoren Informationstechnik und Telekommunikation sollten, sofern sie vom Anwendungsbereich des NIS2-Umsetzungsgesetzes bereits erfasst sind, vollständig aus dem Anwendungsbereich des KRITIS-Dachgesetz herausgenommen werden. Entsprechend der EU-rechtlichen Vorgaben gelten gemäß § 4 Abs 6 des Entwurfs die §§ 7 bis 12 nicht für verschiedene Sektoren. Übrig bleibt letztlich die Registrierungspflicht nach § 6 des Entwurfs. Diese findet sich aber bereits in der NIS2 und dem entsprechenden Umsetzungsgesetz. Insofern können die Sektoren auch von vornherein komplett ausgenommen werden. Durch die teilweise Herausnahme aus dem Anwendungsbereich entstehen rechtliche Unklarheiten, die vermieden werden könnten.

Unklar erscheint Unternehmen die genaue Implikation des Vorrangs, den das Gesetz bereits anzuwendenden Spezialvorschriften beimitst (§ 4 Abs 7, 8). Es wäre nicht nachvollziehbar, wenn Pflichten zur gesonderten Dokumentation der getroffenen Maßnahmen weiter bestehen – statt eines einfachen Verweises auf bestehende Auditierung, beispielsweise nach dem LuftSiG.

Insbesondere für Zulieferer der verpflichteten Betreiber, z. B. IT-Dienstleister, bestehen weiterhin Unklarheiten in Bezug auf die eigene Betroffenheit. Dazu sollte die Rechtsverordnung nach § 16 Abs 1 konkretisierende Ausführungen enthalten.

### **Behördenzuständigkeit und Zusammenarbeit der Behörden (§ 3)**

Das BBK ist zuständige Behörde im Hinblick auf Aufgaben des Bundes. Neu vorgesehen ist, dass (neben weiteren Sektorbehörden des Bundes) auch Behörden der Länder für bestimmte Betreiber, Dienstleistungen und Sektoren zuständig sind.

Die Einbeziehung der Länder in die Umsetzung stößt bei den Unternehmen auf geteiltes Echo. So steht einer vermuteten größeren Nähe zu den Unternehmen, und damit einfacheren Austausch- und Kooperationsprozessen, die vielfach geäußerte Befürchtung gegenüber, dass die Zuständigkeit unterschiedlicher Landesbehörden auch zu unterschiedlicher Behördenpraxis

führen wird. Die beabsichtigte Teilung der Zuständigkeiten zwischen Bundes- und Länderbehörden ist so auszugestalten, dass klare Zuständigkeiten definiert werden und einer bundesweit einheitlichen Handhabung nichts entgegensteht.

Unternehmen bezweifeln zudem, dass länderspezifische Behörden in der Lage sein werden, einheitliche Anforderungen an die Betreiber zu stellen. So ist vorgesehen, dass Bundesländer branchenspezifische Resilienzstandards erlassen, wenn bis zum 01.01.2029 noch keine Rechtsverordnungen für einzelne Sektoren durch das BBK (im Einvernehmen mit Sektorbehörden des Bundes und im Benehmen mit den Länderbehörden) als geeignet anerkannt wurden. Dies würde z. B. auch die Zulieferer von IT-Dienstleistungen für KRITIS-Betreiber betreffen, weil daraus unterschiedliche Anforderungen an Softwarelösungen je nach Bundesland resultieren können, was den Komplexitätsgrad dieser Lösungen – und damit die Kosten – enorm erhöhen würde.

Uneinigkeiten zwischen den Behörden von Bund und Ländern bei der Etablierung von Resilienzstandards dürfen nicht dazu führen, dass Unternehmen aufgrund nicht vorhandener Verordnungen von Beginn an rechtsunsicher sind und sich ab 2029 ein Flickenteppich von regionalen Regelungen bildet. Insofern sollte darauf hingewirkt werden, deutlich früher als zum 17.07.2026 (Umsetzungsfrist für Resilienzmaßnahmen bei Betreibern) bundeseinheitliche, besser noch EU-weit gültige, Rechtsverordnungen vorliegen zu haben.

### **Registrierung kritischer Anlagen (§ 6)**

Die Betreiber kritischer Anlagen sollen diese spätestens drei Monate nach Erfüllung der Betroffenheitskriterien über ein gemeinsames Online-Meldeportal von BBK und BSI registrieren und eine Kontaktstelle bzw. Ansprechperson benennen, die jederzeit erreichbar ist.

Das Portal sollte auch Prüfmöglichkeiten enthalten, anhand derer die Unternehmen ihre Betroffenheit vor der Registrierung als Self-Service einfach selber überprüfen können. Bestehende Registrierungen nach BSIG sollten für die Registrierungen nach § 8 Kritis-Dachgesetz ohne erneute Registrierung anerkannt und übernommen werden.

### **Nationale Risikoanalysen und Risikobewertungen der Unternehmen (§§ 8, 9)**

Die für die jeweiligen kritischen Dienstleistungen zuständigen Bundes- und Landesministerien müssen alle vier Jahre oder auf Veranlassung Risikoanalysen und -bewertungen durchführen. Das BBK legt darüber hinaus methodische und inhaltliche Vorgaben dafür durch Verwaltungsvorschrift fest, wertet die Risikoanalysen und -bewertungen sektorenübergreifend aus und stellt relevante Teile den Betreibern, Länder- und Bundesbehörden zur Verfügung. Die Betreiber wiederum müssen auf dieser Grundlage und weiterer Informationen erstmals zum 17. Juli 2026 und dann alle vier Jahre eigene Risikoanalysen durchführen. Dafür kann das BBK Vorgaben machen und Vorlagen und Muster bereitstellen.

Der Ansatz einer doppelten Risikoanalyse und Risikobewertung aus staatlicher und aus unternehmerischer Perspektive ist grundsätzlich unterstützenswert. Die Vorgaben dafür wurden im Gesetzentwurf konkretisiert. Eine vierjährige Aktualisierung wird den sich sehr dynamisch entwickelnden Bedrohungsszenarien sowie den technologischen Rahmenbedingungen und Entwicklungen nicht gerecht. Insofern ist eine Initiierung „auf Veranlassung“ richtig. Es stellt sich allerdings weiterhin die Frage, was genau damit gemeint ist. Obwohl missverständlich, könnte es durchaus sogar sachdienlich sein, wenn damit sowohl „anlassbezogen“ (beispielsweise aufgrund eines externen Ereignisses) als auch als „veranlasst“ im Sinne „von den zuständigen Stellen angefordert“ gemeint sein kann. Bei Letzterem wäre zu definieren, ob eine (aktualisierte) Risikobewertung durch ein Bundes- bzw. Landesministerium oder Branchenverbände, UP KRITIS etc.veranlasst werden soll. In den Risikoanalysen sollten auch Erfahrungen aus vergangenen Notlagen einfließen.

### **Resilienzplan und Resilienzmaßnahmen der Betreiber kritischer Anlagen (§ 10)**

Die Betreiber kritischer Anlagen müssen auf Basis der Risikoanalysen und -bewertungen Resilienzmaßnahmen nach dem Stand der Technik umsetzen. Die Umsetzungsfrist dafür beträgt 10 Monate nach ihrer Registrierung. Neu im Entwurf ist eine Auflistung beispielhafter Maßnahmen. Ein Katalog von sektorenübergreifenden Mindestanforderungen stellt das BBK auf seiner Internetseite zur Verfügung. Die Betreiber müssen die Maßnahmen in einem Resilienzplan darstellen, in dem die Erwägungen bei der Auswahl der Maßnahmen und Risikoanalysen dargelegt werden. Auch dafür kann das BBK Vorlagen und Muster bereitstellen.

Positiv ist, dass das BBK zur Unterstützung der Betreiber Vorlagen und Muster zur Verfügung stellen wird. Ergänzende Hinweise beispielsweise zu der Frage, wie die Redundanz in den Lieferketten sinnvollerweise aussehen soll, sind sicherlich hilfreich. So ist die Einführung komplexer Scada-Systeme zur Steuerung von Energienetzen aufwändig und langwierig. Es sollte nicht gemeint sein, dass die Unternehmen auch in solchen Fällen schnell den Lieferanten insgesamt wechseln können müssen. Die Forderung nach Redundanz sollte hier beispielsweise bedeuten, dass ein ersatzbedürftiges Teilsystem entweder offen ist für Reparaturen/Anpassungen, oder aber, dass es an den kritischen Punkten durch eine andere Teil- oder Zwischenlösung überbrückt werden können muss.

Unternehmen schätzen die 10-Monatsfrist zum Treffen geeigneter Resilienzmaßnahmen als zu kurz ein. Bereits Beschaffungsprozesse für eventuelle Komponenten und Systeme können hier länger dauern. Eine 2-Jahresfrist entspricht den praktischen Bedingungen eher.

### **Nachweise (§ 11)**

Betreiber müssen die Umsetzung der Resilienzmaßnahmen nur noch auf Nachfrage gegenüber der jeweils zuständigen Behörde nachweisen, nicht mehr zwingend alle zwei Jahre. Diese Praxisorientierung unterstützen wir.

## **Meldungen von Vorfällen (§ 12)**

Das Meldewesen wurde umfassend überarbeitet. Betreiber kritischer Anlagen sollen Vorfälle, die die Erbringung kritischer Dienstleistungen erheblich stören oder erheblich stören könnten, unverzüglich an eine vom BBK und BSI eingerichtete gemeinsame Meldestelle melden. Eine Erstmeldung soll bis spätestens 24 Stunden nach Kenntnis des Vorfalls erfolgen und spätestens einen Monat danach ein ausführlicher Bericht abgegeben werden. Das BBK veröffentlicht Details zum Meldeverfahren und den Inhalten der Meldungen auf seiner Internetseite. Es übermittelt den zuständigen Aufsichtsbehörden von Bund und Ländern Auswertungen zu Meldungen von Vorfällen.

Für bürokratiearme Prozesse sollte nur eine Meldung über das Portal des BSI erforderlich sein, deren Umfang klar definiert werden muss. Zu prüfen wäre, inwiefern auch bereits bestehende Meldeverpflichtungen gegenüber anderen Stellen über dieses Meldeportal abgewickelt werden können. Für die Weiterverteilung der Informationen an andere Behörden sind effektive technische und organisatorische Prozesse zu definieren und auf ein angemessenes Schutzniveau sensibler Informationen zu achten. Unternehmen regen an, hier analog zu BSIG § 5 Abs 4, 5 zu definieren, dass der Umgang mit den Informationen im Sinne des Geheimschutz erforderlich ist.

Die Meldungen von Sicherheitsvorfällen müssen so aufbereitet sein, dass nicht nur an den von einem Vorfall betroffenen Betreiber „sachdienliche Folgeinformationen“, z. B. Leitlinien, übermittelt werden (§ 12 Abs 7), sondern weitere potenziell gefährdete Betreiber kritischer Dienstleistungen gezielt Warnhinweise erhalten. Wir verweisen an dieser Stelle auf unsere Ausführungen zum Entwurf vom Sommer 2023: Die meldenden Unternehmen erwarten, dass sie auch einen konkreten Mehrwert im Sinne eines „Rückkanals“ haben, indem sie zielgerichtet aktuelle Informationen zur Gefährdungslage erhalten.

## **Unterstützung der Betreiber kritischer Anlagen (§ 13)**

Positiv ist, dass das BBK Betreibern kritischer Anlagen Vorlagen, Muster und Leitlinien für die Umsetzung zur Verfügung stellt und dass es auch Beratungen, Schulungen und Übungen anbieten kann. Es sollte dies umfassend und entsprechend den Bedarfen der Betreiber umsetzen.

## **Geschäftsleiterverantwortung (§ 14)**

Entsprechend dem Entwurf des NIS2UmsuCG sieht auch der vorliegende Entwurf nun vor, dass Geschäftsleiter von Betreibern die Resilienzmaßnahmen billigen und die Umsetzung überwachen müssen. Ebenso müssen sie regelmäßig an Schulungen teilnehmen und auf Nachfrage Nachweise vorlegen.



Die Pflicht zur ordnungsgemäßen Unternehmensleitung umfasst grundsätzlich auch physische Maßnahmen zur Sicherheit. Insofern ist die Verankerung der Verantwortung für die Risiko-maßnahmen nach § 10 in der Unternehmensführung im Gesetzentwurf grundsätzlich richtig – aber nicht erforderlich. Wir regen eine Streichung des § 14 Abs 1 Satz 2 an, der einen Verzicht des Betreibers auf Ersatzansprüche bzw. einen Vergleich ausschließt. Auch hier sollte man sich an allgemeinen Grundsätzen orientieren.

Für Leiter nationaler Unternehmensteile von internationalen Konzernunternehmen, deren IT-Systeme in der Regel zentral betrieben und überwacht werden, haben nationale Geschäftsleiter keinen Einfluss auf wesentliche Aspekte des Risikomanagements. Insofern würde dieser Regelung für die Betroffenen unbillige Haftungsrisiken bedeuten. Auch bei der Abwehr physischer Gefahren bestehen i.d.R. unternehmensweite Standards, oder es kommen bereits gesetzliche Vorschriften zu Umsetzung. Gerade im letzteren Fall erübrigt sich, dass Geschäftsleiter Maßnahmen billigen (weil sie spezialrechtlich vorgeschrieben sind) oder überwachen (weil dies der jeweils zuständigen Aufsichtsbehörde obliegt). Konkret ist keine Veranlassung erkennbar, weshalb ein Geschäftsleiter zusätzlich zur mit der Umsetzung von „Spezialvorschriften“ (bspw. LuftSiG) betrauten Fachabteilung eine zusätzliche Rolle bzw. Obliegenheit haben sollte. Womöglich wäre hier mindestens ein Halbsatz in § 14 zur Klarstellung nützlich („...,mit Ausnahme solcher Maßnahmen gemäß § 4 Abs 7,“).

### **Ausnahmebescheid (§ 17)**

Vor allem für Sicherheitsbehörden gibt es Abweichungen und Ausnahmebescheide zu den Maßnahmen.

Die Herausnahme der o. g. Stellen aus dem Geltungsbereich des Gesetzes ist nachvollziehbar, wenn bereits vergleichbare Vorgaben bestehen. Allerdings sollten Störungen (§ 12) entweder auch durch diese Stellen an das zentrale Portal gemeldet werden, oder sichergestellt werden, dass die relevanten Informationen dazu ebenfalls dem BBK zur Verfügung gestellt werden, um ein umfassendes Lagebild für die Betreiber kritischer Infrastrukturen zu generieren.

Grundlage dieser Stellungnahme sind die der DIHK bis zur Abgabe der Stellungnahme zugegangenen Äußerungen der IHKs sowie die wirtschaftspolitischen/europapolitischen Positionen sowie insbesondere die Beschlüsse des DIHK Vorstandes vom 27. Juni 2018 „Daten- und Informationssicherheit – Vertrauen nachhaltig gewährleisten“ und des DIHK-Präsidiums vom 22. Juni 2023 „Netze – Lebensadern der Wirtschaft: Netzausbau in Deutschland bedarfsgerecht, sicher und nachhaltig gestalten“. Sollten der DIHK noch weitere in dieser Stellungnahme noch nicht berücksichtigte relevante Äußerungen zugehen, wird die DIHK diese Stellungnahme entsprechend ergänzen.



## **Ansprechpartnerin**

Dr. Katrin Sobania, [sobania.katrin@dihk.de](mailto:sobania.katrin@dihk.de), Tel. 030/20308-2109

## **Wer wir sind:**

Unter dem Dach der Deutschen Industrie- und Handelskammer (DIHK) sind die 79 Industrie- und Handelskammern (IHKs) zusammengeschlossen. Unser gemeinsames Ziel: Beste Bedingungen für erfolgreiches Wirtschaften.

Auf Bundes- und Europaebene setzt sich die DIHK für die Interessen der gesamten gewerblichen Wirtschaft gegenüber Politik, Verwaltung und Öffentlichkeit ein.

Denn mehrere Millionen Unternehmen aus Handel, Industrie und Dienstleistung sind gesetzliche Mitglieder einer IHK - vom Kiosk-Besitzer bis zum Dax-Konzern. So sind DIHK und IHKs eine Plattform für die vielfältigen Belange der Unternehmen. Diese bündeln wir in einem verfassten Verfahren auf gesetzlicher Grundlage zu gemeinsamen Positionen der Wirtschaft und tragen so zum wirtschaftspolitischen Meinungsbildungsprozess bei.