

## **Mandanteninformation 15/2025**

### **Strenge Sicherheitsvorgaben für Einrichtungen durch NIS2 und Co.**

Für zehntausende Einrichtungen, insbesondere auch der Abfall-, Energie und Wasserwirtschaft, gelten seit dem 06.12.2025 deutlich strengere Vorgaben zur IT-Sicherheit, etwa Melde- und Registrierungspflichten sowie neue Anforderungen an das Risikomanagement. Denn seit diesem Zeitpunkt gilt das Gesetz zur Umsetzung der NIS2-Richtlinie, welches unter anderem ein neues BSI-Gesetz enthält. Bei Verstößen drohen hohe Bußgelder. Im Laufe des Jahres 2026 wird es zudem erstmals Anforderungen an die physische Widerstandsfähigkeit (Resilienz) geben; das geplante KRITIS-Dachgesetz zur Umsetzung der CER-Richtlinie wird derzeit im Bundestag beraten.

### **Bisher: Nur Kritische Infrastrukturen betroffen**

Bislang hatte das Cybersicherheitsrecht einen engen Anwendungsbereich: Seit dem IT-Sicherheitsgesetz aus dem Jahr 2015 mussten vor allem Kritische Infrastrukturen, also Anlagen von hoher Bedeutung für das Funktionieren des Gemeinwesens, angemessene organisatorische und technische Vorkehrungen treffen, damit die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der IT gewährleistet ist. Insbesondere ging es hierbei um die Abwehr von Cyberangriffen.

In Deutschland sind aktuell mehr als 2.100 Kritische Infrastrukturen beim Bundesamt für Sicherheit in der Informationstechnik (BSI) registriert. Darunter fallen die in der Verordnung zur Bestimmung Kritischer Infrastrukturen (BSI-KritisV) gelisteten Anlagen, bei denen der dort genannte Schwellenwert erreicht oder überschritten wird, beispielsweise Abfallbehandlungsanlagen mit einer Kapazität zur Behandlung von Restabfall von mindestens 79.500 Tonnen pro Jahr.

### **Aktuell: Gesetz zur Umsetzung der NIS-2-Richtlinie**

Das neue IT-Sicherheitsrecht betrifft viel mehr Einrichtungen und enthält konkretere Anforderungen. Das „Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung“ tritt am 06.12.2025 in

Kraft. Kernstück der Umsetzung der NIS2-Richtlinie (EU) 2022/2555 ist eine umfangreiche Novelle des BSI-Gesetzes.

### **Akteure der Privatwirtschaft und der öffentlichen Hand betroffen**

Rund 30.000 „besonders wichtige“ und „wichtige“ Einrichtungen fallen in den Anwendungsbereich des neuen BSI-Gesetzes (§§ 28 ff.), das im Gesetz zur Umsetzung der NIS2-Richtlinie enthalten ist. Zusätzlich sind die Zulieferer der genannten Einrichtungen indirekt betroffen, da Letztere verpflichtet sind, für Sicherheit in der Lieferkette zu sorgen. Für die Bundesverwaltung gibt es eigene Bestimmungen.

Die strengsten Regelungen gelten für „besonders wichtige“ Einrichtungen. Dies umfasst neben Kritischen Infrastrukturen (die fortan „kritische Anlagen“ heißen) unter anderem alle Unternehmen, die den in Anlage 1 des BSI-Gesetzes genannten Sektoren wie etwa Trinkwasserversorgung oder Abwasserbeseitigung angehören. Hiervon ausgenommen sind kleine oder mittlere Unternehmen (KMU), die zum einen weniger als 250 Personen beschäftigen und zum anderen einen Jahresumsatz von höchstens EUR 50 Mio. erzielen oder deren Jahresbilanzsumme sich auf höchstens EUR 43 Mio. beläuft, wobei die Daten von Gesellschaftern und Beteiligungen eventuell zu berücksichtigen sind.

Für die Einordnung als „wichtige“ Einrichtung genügt es, wenn das Unternehmen den in Anlage 1 oder Anlage 2 des BSI-Gesetzes genannten Sektoren unterfällt, was z.B. alle Unternehmen der Abfallbewirtschaftung (§ 3 Ab. 14 des Kreislaufwirtschaftsgesetzes, KrWG) erfasst. Hierbei sind KMU nicht generell ausgenommen. Die Schwelle ist niedriger angesetzt: Auch mittlere Unternehmen mit mindestens 50 Mitarbeitern oder mit sowohl Jahresumsatz als auch Jahresbilanzsumme von über EUR 10 Mio. können daher wichtige Einrichtungen sein.

Über Unternehmen der Privatwirtschaft hinaus werden auch Anstalten und Körperschaften des öffentlichen Rechts erfasst. Hierbei werden Eigenbetriebe als selbstständige Organisationseinheiten behandelt, so dass die IT betroffener Eigenbetriebe von den Systemen anderer Kommunalbetriebe abgekoppelt werden muss.

### **Anforderungen an die Cybersicherheit**

Alle „besonders wichtigen“ und „wichtigen“ Einrichtungen müssen sich beim BSI registrieren und Risikomanagementmaßnahmen einführen, die u.a. Konzepte, Schulungen, Backup-Management und Multi-Faktor-Authentifizierung beinhalten. Sicherheitsmaßnahmen müssen dem Stand der Technik entsprechen. In der Praxis helfen die bereits in vielen Branchen bestehenden Standards, darunter der neue branchenspezifische Sicherheitsstandard für die Siedlungsabfallentsorgung (B3S SAE).

Bei erheblichen Sicherheitsvorfällen greift künftig ein dreistufiges Meldesystem mit knapp bemessenen Fristen: Erstmeldung (24 Stunden),

Detailbericht (72 Stunden) und Abschlussmeldung zu den ergriffenen Abhilfemaßnahmen etc. (1 Monat). Zusätzlich zur Meldung an die Behörde kann das BSI diese Einrichtungen auch dazu verpflichten, die Kunden über den Vorfall zu informieren.

Cybersicherheit ist zukünftig Chefsache. Die Geschäftsleitung wird durch das Gesetz direkt adressiert und kann seine Verantwortung nicht auf Beauftragte delegieren. Sie muss regelmäßig an Schulungen teilnehmen und haftet bei Verstößen nach den für die betreffende Rechtsform vorgesehenen Bestimmungen. Das neue BSI-Gesetz zwingt damit viele Akteure zum Umdenken bei der Governance in Fragen der IT-Sicherheit.

### **Hohe Bußgelder**

Das neue BSI-Gesetz sanktioniert Verstöße gegen die neuen Vorgaben mit empfindlichen Bußgeldern. Das gilt insbesondere, soweit „besonders wichtige“ Einrichtungen betroffen sind: Je nach Tatbestand können hier Bußgelder bis zu EUR 10 Mio. sowie bis zu 2% des weltweit erzielten Jahresumsatzes verhängt werden.

Insgesamt bekommt das BSI als zentrale Cybersicherheitsbehörde mehr Kompetenzen für Aufsichts- und Durchsetzungsmaßnahmen. Beispielsweise kann es „besonders wichtigen“ Einrichtungen zu Audits oder Zertifizierungen verpflichten. Zugleich fungiert das BSI in der koordinierenden Funktion des Chief Information Security Officer (CISO) als zentrale Stelle für die Cybersicherheit der Bundesverwaltung.

### **Ausblick: KRITIS-Dachgesetz zur Umsetzung der CER-Richtlinie**

Parallel zur Novelle des BSI-Gesetzes kommt ein weiteres Gesetz, das die CER-Richtlinie (EU) 2022/2557 über die Resilienz kritischer Einrichtungen umsetzt und einen komplett neuen Rechtsakt enthält: das KRITIS-Dachgesetz. Im Vordergrund steht dort nicht die Cybersicherheit, sondern die physische Resilienz. Als zentrale Anlaufstelle für die physische Resilienz ist nicht das BSI, sondern das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) vorgesehen. Der Anwendungsbereich der beiden Gesetzesvorhaben weicht voneinander ab, so dass manche Einrichtungen nur unter eines der beiden neuen Gesetze fallen und andere sowohl die Vorgaben für die IT-Sicherheit als auch die Anforderungen an die physische Resilienz zu erfüllen haben.

Zum Entwurf des „Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen“ fand am 01.12.2025 eine Anhörung im Innenausschuss des Bundestages statt, bei der insbesondere kritisiert wurde, die beiden Gesetzentwürfe seien nicht hinreichend aufeinander abgestimmt und die Resilienzvorgaben für staatliche Stellen gingen nicht weit genug. Noch nicht abzusehen ist, ob das KRITIS-Dachgesetz bereits Mitte 2026 in Kraft treten wird. Denn es bedarf der Zustimmung des Bundesrates, der bereits in einer ersten Stellungnahme

Änderungen angemahnt hatte. Wir werden über den weiteren Gesetzgebungsprozess zum KRITIS-Dachgesetz berichten.

06. Dezember 2025

okl & partner  
Rechtsanwälte PartG mbB

Büro Köln  
Von-Werth-Straße 2 | 50670 Köln  
T: +49 (0) 221 | 42 07-0  
koeln@oklp.de

Büro Berlin  
Jägerstraße 54-55 | 10117 Berlin  
T: +49 (0) 30 | 2577112-0  
berlin@oklp.de

[www.oklp.de](http://www.oklp.de)