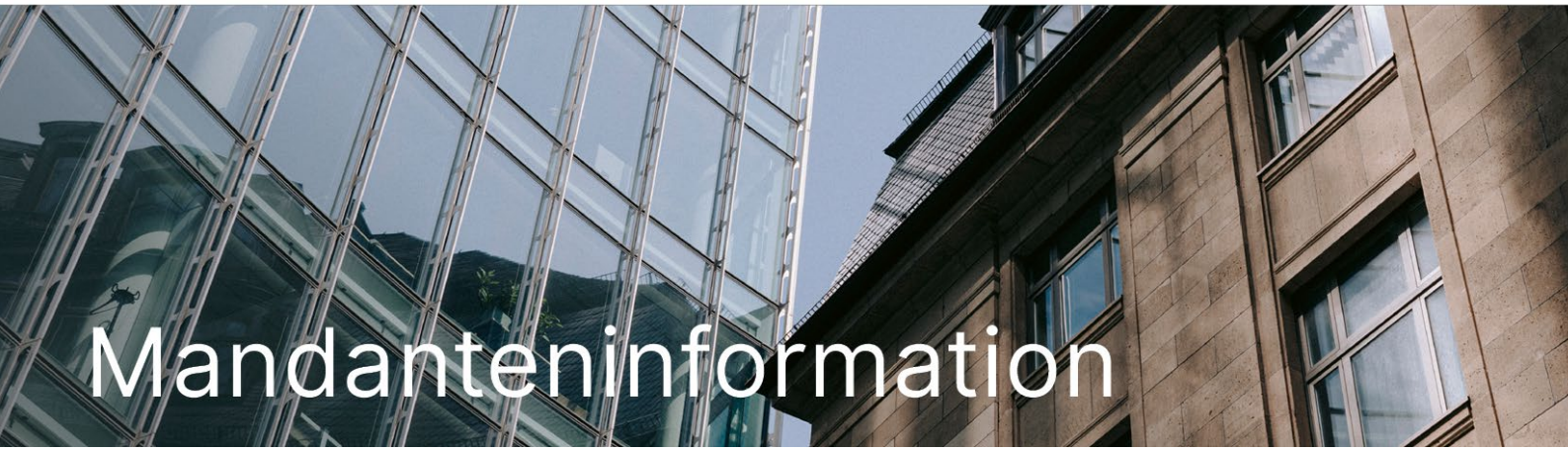

Mandanteninformation

August 2026

Update zur Cybersicherheit: Änderungsvorschläge der NIS2-Richtlinie und Entwurf eines neuen Cybersecurity Acts

Die Europäische Kommission hat im Frühjahr 2026 ein Cybersecurity-Paket vorgelegt, das sowohl bestimmte Änderungen der NIS2-RL als auch den Entwurf eines neuen Cybersecurity Acts (CSA 2) umfasst. Während die Änderungen der NIS2-RL vor allem auf Klarstellung und Vereinfachung abzielen, soll der neue CSA 2 einen einheitlichen Rahmen für die Sicherheit von Lieferketten im Bereich der Informations- und Kommunikationstechnologie (IKT) und für die Cybersicherheitszertifizierung schaffen, der für betroffene Unternehmen zusätzliche Anforderungen mit sich bringen kann.

I. Zielrichtung der Reform: Vereinfachung und Harmonisierung

Die Kommission möchte die bislang als administrativ belastend angesehene Umsetzung der NIS2-RL vereinfachen und zugleich stärker vereinheitlichen. Das Cybersecurity-Paket soll das Zusammenspiel der NIS2-RL mit dem Entwurf eines neuen CSA 2 und sektorspezifischen Rechtsakten verbessern. Der Reformansatz zielt damit auf Verfahrensvereinfachung und stärkere Kohärenz, soll aber zugleich auch das Cybersicherheitsniveau in der Union stärken.

Im Mittelpunkt steht eine stärker vereinheitlichte Ausgestaltung des Cybersicherheitsrechts. Nationale Abweichungen sollen zurückgedrängt, europäische Zertifizierungsmechanismen und koordinierte Aufsichtsstrukturen gestärkt werden. Während die Änderungen der NIS2-RL vor allem punktuelle Klarstellungen und Vereinfachungen vorsehen, etabliert der CSA 2 mit dem unionsweiten Rahmen für vertrauenswürdige IKT-Lieferketten auch weitergehende Anforderungen an das Lieferkettenmanagement.

Änderungen der NIS2-RL[1]

1. Anwendungsbereich

Die Kommission schlägt mehrere punktuelle, aber praxisrelevante **Klarstellungen zum persönlichen Anwendungsbereich der NIS2-RL** vor. Unter anderem werden Betreiber von Unterseedatenübertragungsinfrastruktur, einschließlich landseitiger Anbindungen und zugehöriger Betriebsinfrastruktur als wesentliche Einrichtungen erfasst (Anhang I Ziffer 8 NIS2-RL n.F.). Nach der Begründung der Kommission soll damit eine Regelungslücke geschlossen werden, weil die NIS2-RL diese strategisch bedeutsame Infrastruktur bislang nicht vollständig erfasse (Erwägungsgrund 6 NIS2-ÄndRL). Zudem werden bestimmte Sektoren – u. a. Gesundheitswesen, Energieerzeugung, Wasserstoffwirtschaft und chemische Industrie – näher abgegrenzt, um Auslegungsunsicherheiten zu reduzieren (Anhang I Ziffern 1a, 1e, 5; Anhang II Ziffer 3 NIS2-RL n.F.).

Praxishinweis: Der Anwendungsbereich der NIS2-Pflichten ist in Deutschland in § 28 BSIG geregelt. Neben den in Anlagen 1 und 2 BSIG aufgeführten Einrichtungen fallen insbesondere Betreiber kritischer Anlagen in den sektoralen Anwendungsbereich der NIS2-Pflichten. Im Mai 2026 ist ein Referentenentwurf zur KritisVO[2] bekannt geworden, der detaillierte Bestimmungen zur Konkretisierung der kritischen Anlagen nach § 28 BSIG enthält.

Neu eingeführt wird ferner eine Unternehmenskategorie sogenannter **„small mid-caps“**. Diese umfasst Unternehmen, die weniger als 750 Personen beschäftigen und einen Jahresumsatz von höchstens 150 Mio. EUR erzielen oder deren Jahresbilanzsumme sich auf höchstens 129 Mio. EUR beläuft (Art. 6 Nr. 2 NIS2-RL n.F.). Small mid-caps sollen zwar weiterhin in den Anwendungsbereich der NIS2-RL fallen, wenn sie in den von der Richtlinie erfassten Sektoren tätig sind. Sie sollen jedoch als „wichtige“ und nicht als „wesentliche“ Einrichtungen eingestuft werden, um den Compliance-Aufwand zu begrenzen (Art. 3 Abs. 1 lit. a, Abs. 2 NIS2-RL n.F.).

Praxishinweis: Nach der derzeitigen deutschen Umsetzung im BSIG gelten für wichtige und besonders wichtige Einrichtungen – letztere entsprechen in der Terminologie der NIS2-RL den wesentlichen Einrichtungen – grundsätzlich dieselben Kernpflichten.[3] Diese umfassen insbesondere:

- Risikomanagementmaßnahmen, § 30 BSIG
- Melde-, Registrierungs-, und Unterrichtungspflichten, §§ 32-35 BSIG
- Umsetzungs-, Überwachungs- und Schulungspflichten der Geschäftsleitung, § 38 BSIG

Die Kategorisierung als „wichtige“ oder „besonders wichtige Einrichtung“ kann sich auf den **Umfang der durchzuführenden Risikomanagementmaßnahmen** auswirken, da diese in einem angemessenen Verhältnis zur Risikoexposition der Einrichtung stehen müssen, § 30 Abs. 1 BSIG.

2. Harmonisierung technischer Sicherheitsanforderungen

Von praktischer Tragweite ist auch der Vorschlag, die technischen und methodischen Anforderungen an Risikomanagementmaßnahmen künftig stärker **durch unionsweit verbindliche Durchführungsrechtsakte** zu konkretisieren. Nach Erlass entsprechender Durchführungsrechtsakte sollen die Mitgliedstaaten keine abweichenden oder weitergehenden nationalen Anforderungen mehr vorsehen

[1] https://digital-strategy.ec.europa.eu/de/library/proposal-directive-regards-simplification-measures-and-alignment-cybersecurity-act

[2] abrufbar unter: https://ag.kritis.info/wp-content/uploads/2026/05/260526_Entwurf-Kritisverordnung.pdf

[3] https://www.sza.de/assets/downloads/2026-01-05-SZA-Mandanteninformation-Nis2-CRA.pdf

dürfen (Art. 21 Abs. 5 UAbs. 5 i.V.m. Art. 5 NIS2-RL n.F.).

Damit werden nationale Sonderwege – etwa bei der Ausgestaltung technischer Sicherheitsmaßnahmen – erheblich eingeschränkt. Derzeit sieht Art. 5 NIS2-RL vor, dass die Mitgliedstaaten grundsätzlich nicht daran gehindert sind, Bestimmungen zu erlassen oder beizubehalten, die ein höheres Cybersicherheitsniveau gewährleisten als die unionsrechtlichen Durchführungsrechtsakte. Auf nationaler Ebene eröffnet § 30 Abs. 5 BSIG unter gewissen Voraussetzungen die Möglichkeit, über die NIS2-RL hinausgehende Cybersicherheitsmaßnahmen anzuordnen.

3. Lieferkettensicherheit

Die Kommission greift ausdrücklich die in der Praxis vielfach geäußerte Kritik an heterogenen und **umfangreichen Lieferketten-Fragebögen** auf. Künftig sollen Leitlinien der Kommission einheitliche Struktur-, Format- und Detailvorgaben für entsprechende Informationsabfragen enthalten (Erwägungsgrund 9 NIS2-ÄndRL).

4. Meldungen und Informationspflichten

Die Kommission schlägt eine unionsweit **harmonisierte Erhebung von Informationen zu Ransomware-Angriffen** vor. Künftig soll daher auf Anfrage auch verpflichtend anzugeben sein, ob und ggf. in welcher Höhe und an wen Lösegeldzahlungen geleistet wurden (Art. 23 Abs. 12, 13 NIS2-RL n.F.).

Bestimmte Einrichtungen sollen zudem eine **schnellere Aktualisierung ihrer besonderen Registrierungspflichten** (derzeit geregelt in § 34 BSIG) vornehmen müssen, sofern sich die an das BSI zu übermittelnden Angaben ändern. Dies betrifft die in § 60 Abs. 1 BSIG genannten Einrichtungen, etwa Anbieter von Rechenzentrumsdiensten, Online-Marktplätzen und Plattformen für soziale Dienste. Die bisherige Frist von drei Monaten (§ 34 Abs. 2 BSIG) soll auf zwei Wochen verkürzt werden (Art. 27 Abs. 3 NIS2-RL n.F.). Diese zweiwöchige Frist galt bislang schon mit Blick auf die weniger weitreichende Registrierungspflicht nach § 33 BSIG, die auf alle der NIS2-RL unterfallende Unternehmen Anwendung findet (§ 33 Abs. 5 BSIG).

5. Stärkung der Rolle von ENISA

Die EU-Cybersicherheitsagentur ENISA soll künftig eine stärkere Rolle bei der Koordinierung der Aufsicht über grenzüberschreitend tätige Unternehmen übernehmen. Art. 27 Abs. 1 NIS2-RL n.F. sieht u. a. ein **zentrales Register aller unter NIS2 fallenden Unternehmen** vor (bislang bezieht sich das Register nur auf bestimmte Kategorien von Einrichtungen). Zudem sieht die NIS2-ÄndRL Unterstützungsleistungen ENISAs im Rahmen grenzüberschreitender Aufsichtstätigkeiten vor (Art. 37a NIS2-RL n.F.).

II. Neuer Cybersecurity Act[4]

1. Lieferkettensicherheit

Titel IV des CSA 2 etabliert erstmals einen EU-weit einheitlichen Rahmen zur Absicherung sogenannter „**trusted ICT supply chains**“. Adressiert werden nicht primär technische Schwachstellen einzelner Produkte, sondern strukturelle Risiken, die sich insbesondere aus der Herkunft von Lieferanten aus Drittstaaten ergeben, von denen Wirtschaftsspionage, Cyberangriffe oder staatlich gesteuerte Kampagnen gegen die Union oder ihre Mitgliedstaaten ausgehen (Erwägungsgrund 129 CSA 2). Der Anwendungsbereich der trusted ICT supply chains erfasst Unternehmen in hoch-kritischen und kritischen Sektoren im Sinne der Anhänge I und II der NIS2-RL, etwa in Bereichen Energie, Telekommunikation, Gesundheitswesen, Verkehr und digitale Infrastruktur (Art. 98 Abs. 1 CSA 2).

Die Kommission soll befugt werden, **Drittstaaten als Staaten mit erheblichen Cybersicherheitsrisiken** einzustufen (Art. 100 CSA 2). Maßgeblich sind dabei unter anderem staatliche Einflussmöglichkeiten auf

[4] https://digital-strategy.ec.europa.eu/de/library/proposal-regulation-eu-cybersecurity-act

Unternehmen, fehlende rechtsstaatliche Kontrollmechanismen oder nachgewiesene staatlich gesteuerte Cyberattacken. An diese Einstufung knüpft unmittelbar die Qualifikation von **„Hochrisiko-Anbietern"** an, also Unternehmen, die in solchen Staaten ansässig sind oder unter deren Kontrolle stehen (Art. 2 Nr. 39 CSA 2). Diese Hochrisiko-Anbieter sollen dann unter anderem aus bestimmten EU-Förderprogrammen und öffentlichen Vergabeverfahren ausgeschlossen werden können (Art. 100 Abs. 4 lit. e, f CSA 2).

Darüber hinaus soll die Kommission befugt sein, **bestimmte IKT-Komponenten oder -Systeme als „IKT-Schlüsselkomponenten"** zu definieren (Art. 102 CSA 2). Entscheidend ist, ob diese Komponenten oder Systeme wesentliche und sensible Funktionen für die von den Anhängen I und II NIS2-RL umfassten Einrichtungen erfüllen.

Stammen solche IKT-Schlüsselkomponenten von Hochrisiko-Anbietern, soll die Kommission **deren Einsatz für Unternehmen, die in den Anwendungsbereich der NIS2-RL fallen, untersagen** können (Art. 103 Abs. 1 CSA 2). Die Befugnisse der Kommission sollen aber nicht auf IKT-Schlüsselkomponenten von Hochrisiko-Anbietern beschränkt sein; vielmehr soll sie auch mit Blick auf von anderen Anbietern stammende IKT-Schlüsselkomponenten weitreichende Abhilfemaßnahmen und Verwendungsbeschränkungen anordnen können (Art. 103 Abs. 2, 7 CSA 2).

Für mobile Kommunikationsnetzwerke enthält der CSA 2 bereits eine Definition der IKT-Schlüsselkomponenten, zu denen u.a. Kernfunktionalitäten von 5G-Netzen zählen. Stammen diese Komponenten von Hochrisiko-Anbietern sollen sie schrittweise ersetzt werden (Art. 110 i.V.m. Anhang II Ziffer 1 CSA 2); Einsatz, Verwendung und Installation dieser Komponenten sollen verboten werden (Art. 111 Abs. 1 CSA 2).

Die Durchsetzung der Verpflichtung zur Lieferkettensicherheit soll den bereits nach der NIS2-RL zuständigen Aufsichtsbehörden obliegen (Art. 112 Abs. 1 CSA 2), in Deutschland in der Regel dem BSI. Dazu sollen den Behörden umfangreiche **Aufsichts- und Durchsetzungsbefugnisse** zufallen (Art. 114 CSA 2). Für Verstöße gegen diese Verpflichtungen drohen zudem **empfindliche Bußgelder** in Höhe von bis zu 7 % des weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres (Art. 115 CSA 2).

2. Zertifizierung

Neben diesen lieferkettenbezogenen Pflichten soll der CSA 2 auch den **europäischen Zertifizierungsrahmen für die Cybersicherheit** reformieren. Auch nach geltender Rechtslage können auf Grundlage der von ENISA auszuarbeitenden und von der Kommission für verbindlich zu erklärenden europäischen Schemata für die Cybersicherheitszertifizierung Cybersicherheitszertifikate ausgestellt werden. Sofern nationale oder unionsrechtliche Rechtsakte dies anordnen, sollen diese **Zertifikate als Nachweis dafür dienen können, dass die in diesen Rechtsakten vorgesehenen Cybersicherheitsanforderungen erfüllt sind**. Dies soll jedoch nur gelten, wenn die Zertifizierung von einer Drittstelle vorgenommen wurde (Art. 78 Abs. 2 CSA 2). Entsprechende Regelungen finden sich etwa in Art. 42 Abs. 2 KI-VO und Art. 27 Abs. 8 des Cyber Resilience Acts. Beide Vorschriften sehen bereits nach geltender Rechtslage vor, dass europäische Cybersicherheitszertifikate eine Vermutung der Erfüllung bestimmter, nach diesen Verordnungen bestehender Cybersicherheitsanforderungen begründen können. Eine praktisch bedeutsame Neuerung des CSA 2 ist jedoch die vorgesehene Möglichkeit, nicht nur Produkte, Dienste oder Prozesse, sondern die gesamte **„Cyber Posture" einer Organisation** zertifizieren zu lassen (Art. 71 Abs. 2 lit. c i.V.m. Art. 2 Nr. 29 CSA 2).

3. Ausbau von ENISA

Wie bereits die NIS2-Änd-RL, sieht auch der CSA 2 die Stärkung der Rolle von ENISA vor. ENISA behält zwar ihre unterstützende und beratende Funktion, soll dabei aber insbesondere mehr finanzielle und personelle Ressourcen erhalten.

III. Ausblick und Praxisfolgen

Die Änderungsvorschläge zur NIS2-RL und der Entwurf des CSA 2 unterstreichen die zunehmende Bedeutung von Cybersicherheit auf Unionsebene. Dabei ist für Unternehmen insbesondere die wachsende Fokussierung auf Lieferkettensicherheit von praktischer Relevanz. Die hiermit einhergehenden

Regelungen können dazu führen, dass bestehende Beschaffungs- und Vertragsstrukturen überprüft und gegebenenfalls angepasst werden müssen. Im Vergleich zu den schon bislang bestehenden – anspruchsvollen – Verpflichtungen nach dem BSIG und dem Cyber-Resilience-Act[5] dürfte hiermit eine Ausweitung der von den Unternehmen zu erfüllenden Compliance-Anforderungen verbunden sein. Zugleich gewinnt die europäische Cybersicherheitszertifizierung – auch auf Organisationsebene – als strukturierender Compliance-Baustein weiter an Bedeutung.

Zwar muss das weitere Gesetzgebungsverfahren auf EU-Ebene abgewartet werden. Betroffenen Unternehmen ist dennoch zu empfehlen, sich frühzeitig mit möglichen Risiken in der IKT-Lieferkette auseinanderzusetzen, insbesondere soweit zentrale Komponenten von potenziellen Hoch-Risiko-Anbietern bezogen werden.

Auch auf nationaler Ebene ist ein verstärkter Fokus auf Cybersicherheit erkennbar. Neben dem angesprochenen Referentenentwurf zur KritisVO zeigt dies der im Mai 2026 veröffentlichte Regierungsentwurf eines Gesetzes für Cybersicherheit.[6] Dieser zielt insbesondere auf eine Erweiterung der Aufsichts- und Eingriffsmöglichkeiten von Bundespolizei, BKA und BSI zur Stärkung der staatlichen Cyberabwehr. Vorgesehen sind unter anderem zusätzliche Mitwirkungs- und Auskunftspflichten für Anbieter von öffentlich zugänglichen Telekommunikationsdiensten sowie für geschäftsmäßige Anbieter von digitalen Diensten (§ 15 Abs. 6 BSIG n.F.; § 41a Abs. 9 BPolG n.F.; § 68c Abs. 2 BKAG n.F.). Darüber hinaus sollen Bundespolizei und BKA weitreichendere Befugnisse zur Cyberabwehr erhalten (§ 41a BPolG n.F., § 68a-f BKAG n.F.).

[5] S. hierzu https://www.sza.de/de/thinktank/cyber-resilience-act-pflichten-produkte-mit-digitalen-elementen

[6] https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/CI1/cyberabwehr-regierungsentwurf.pdf?__blob=publicationFile&v=2

Diese Mandanteninformation beinhaltet lediglich eine unverbindliche Übersicht über das in ihr adressierte Themengebiet. Sie ersetzt keine rechtliche Beratung. Als Ansprechpartner zu dieser Mandanteninformation und zu Ihrer Beratung stehen gerne zur Verfügung:

Dr. Thomas Nägele
Rechtsanwalt | Partner
Compliance, Interne Untersuchungen | Datenschutz und Datensicherheit| Gewerblicher Rechtsschutz | IT-Recht | Prozessführung und Schiedsverfahren

T +49 621 4257 222
E Thomas.Naegele@sza.de

Dr. Simon Apel
Rechtsanwalt | Partner
Gewerblicher Rechtsschutz | Datenschutz und Datensicherheit

T +49 621 4257 386
E Simon.Apel@sza.de

Alexander Stolz, LL.M. (Dresden / Exeter)
Rechtsanwalt | Counsel
Commercial | Datenschutz und Datensicherheit| Gewerblicher Rechtsschutz | IT-Recht

T +49 621 4257 222
E Alexander.Stolz@sza.de

Serpil Dilbaz, LL.B.
Rechtsanwältin | Senior Associate
Datenschutz und Datensicherheit| Gewerblicher Rechtsschutz | IT-Recht

T +49 621 4257 222
E Serpil.Dilbaz@sza.de

Hannah Bräunche
Rechtsanwältin | Associate
Gewerblicher Rechtsschutz | Datenschutz und Datensicherheit | Commercial

T +49 621 4257 386
E Hannah.Braeunche@sza.de