Mandanteninformation

Januar 2026

Aktuelle Entwicklungen im Bereich Cybersicherheit: Zum Stand der Umsetzung der NIS2-Richtlinie in Deutschland sowie zum Cyber Resilience Act

Mit mehr als einjähriger Verspätung hat der Bundestag am 13. November 2025 das Gesetz zur Umsetzung der NIS2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationsmanagements in der Bundesverwaltung (NIS2UmsG) beschlossen. Dieses ist am 6. Dezember 2025 in Kraft getreten.[1] Durch Art. 1 NIS2UmsG wird das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSIG) umfassend novelliert und erweitert. Das NIS2UmsG sieht darüber hinaus Änderungen verschiedener Bundesgesetze vor, etwa des Telekommunikationsgesetzes und des Energiewirtschaftsgesetzes.

Am 10. Dezember 2024 ist ein weiterer europäischer Rechtsakt in Kraft getreten, der die Cybersicherheit, konkret die Produktsicherheit, betrifft: Der Cyber Resilience Act (CRA)[2]. Der CRA ist eine europäische Verordnung, die ein Mindestmaß an Cybersicherheit für alle vernetzten Produkte festlegt und ab Ende 2027 voll anzuwenden ist.

A. NIS2UmsG

Das NIS2UmsG sieht neben Berichts-, Informations-, Nachweis- und Registrierungspflichten umfassende verpflichtende Risikomanagementmaßnahmen vor. Diese Pflichten werden durch weitreichende Durchsetzungsmaßnahmen flankiert, die der Umsetzung der NIS2-Richtlinie die erforderliche Schlagkraft verleihen sollen. So etabliert § 38 Abs. 2 BISG eine – subsidiär zu den allgemeinen gesellschaftsrechtlichen Regelungen geltende – Managerhaftung für die Verletzung der Umsetzungs-,

[1] https://www.recht.bund.de/bgbl/1/2025/301/VO.html.

[2] Auch „Cyberresilienz-Verordnung“ genannt, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202402847.

Überwachungs- und Schulungspflichten. Nach § 65 Abs. 5 BISG können zudem auch Geldbußen verhängt werden.

I. Hintergrund

Das NIS2UmsG dient der Umsetzung der NIS2-Richtlinie in nationales Recht. Für Deutschland bedeutet dies, dass der „mit dem Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015 (BGBl. I 2015 S. 1324) und dem Zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0) vom 18. Mai 2021 (BGBl. I 2021, S. 1122) geschaffene Ordnungsrahmen" erweitert sowie entsprechende Vorgaben für die Bundesverwaltung eingeführt werden. Auf Verwaltungsebene zentral ist dabei die Schaffung der Position des Koordinators der Bundesregierung für Informationssicherheit, der das operative Informationssicherheitssystem des Bundes koordiniert und die Ressorts bei der Umsetzung der Vorgaben für das Informationssicherheitsmanagement unterstützt.

II. Adressatenkreis

Der persönliche Anwendungsbereich wird durch das NIS2UmsG entsprechend Art. 2 der NIS2-Richtlinie in Verbindung mit den dazugehörigen Anhängen I und II erweitert. Während in der NIS2-Richtlinie zwischen wichtigen und wesentlichen Einrichtungen unterschieden wird, differenziert das NIS2UmsG zwischen besonders wichtigen Einrichtungen und wichtigen Einrichtungen, vgl. § 28 BSIG.

SZA-Merkkasten: Ob ein Unternehmen in den persönlichen Anwendungsbereich fällt und zu den rund 29.500 durch das BSI beaufsichtigten Einrichtungen gehört, muss von diesem selbst geprüft werden. Zu diesem Zweck wurde vom BSI ein Tool bereitgestellt, mit dem Unternehmen eine NIS2-Betroffenheitsprüfung[3] durchführen können. Diese Prüfung ist jedoch lediglich eine Orientierungshilfe auf Grundlage eigener Angaben und nicht rechtlich bindend. Insbesondere ersetzt sie nicht die Prüfung zur Selbstidentifizierung und hat für eventuelle Verfahren auch keine Indizwirkung. Ihr Unternehmen muss die Betroffenheit daher selbst anhand der nachfolgenden Kriterien beurteilen, die sich sowohl nach der Branche als auch der Größe des Unternehmens richten.

III. Besonders wichtige Einrichtung

Nach § 28 Abs. 1 BSIG ist eine besonders wichtige Einrichtung:

Nr. 1: ein Betreiber kritischer Anlagen, also eine natürliche oder juristische Person oder eine rechtlich unselbstständige Organisationseinheit einer Gebietskörperschaft, die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss auf eine oder mehrere Anlagen ausübt, die den Sektoren Energie, Transport und Verkehr, Finanzwesen, Leistungen der Sozialversicherung sowie der Grundsicherung für Arbeitsuchende, Gesundheitswesen, Wasser, Ernährung, Informationstechnik und Telekommunikation, Weltraum sowie Siedlungsabfallentsorgung angehören und die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, da durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden (§ 28 Abs. 8 iVm § 2 Nr. 22, 24 BSIG); die einzelnen Anlagenarten werden in einer vom Bundesinnenministerium gem. § 56 Abs. 4 BSIG zu erlassenden Rechtsverordnung festgelegt (§ 2 Nr. 22 BSIG).

Nr. 2: ein qualifizierter Vertrauensdiensteanbieter, Top Level Domain Name Registries oder DNS-Diensteanbieter.

Nr. 3: ein Anbieter öffentlich zugänglicher Telekommunikationsdienste oder Betreiber öffentlicher Telekommunikationsnetze mit mindestens 50

[3] https://betroffenheitspruefung-nis-2.bsi.de/.

Mitarbeitern oder einem Jahresumsatz bzw. einer Jahresbilanzsumme von jeweils über 10 Millionen Euro.

Nr. 4: eine sonstige natürliche oder juristische Person oder rechtlich unselbständige Organisationseinheit einer Gebietskörperschaft, die anderen natürlichen oder juristischen Personen entgeltlich Waren oder Dienstleistungen anbietet und die einer der in Anlage 1 bestimmten Einrichtungsarten zuzuordnen ist, und mindestens 250 Mitarbeiter beschäftigt oder einen Jahresumsatz von über 50 Millionen Euro und zudem eine Jahresbilanzsumme von über 43 Millionen Euro aufweist.

Ausgenommen sind Einrichtungen der Bundesverwaltung, sofern sie nicht gleichzeitig Betreiber einer kritischen Anlage sind.

1. Wichtige Einrichtung

Nach § 28 Abs. 2 BSIG ist eine wichtige Einrichtung eine solche, die nicht bereits eine besonders wichtige Einrichtung ist oder zur Bundesverwaltung gehört, aber

Nr. 1: ein Vertrauensdiensteanbieter ist oder

Nr. 2: ein Anbieter öffentlich zugänglicher Telekommunikationsdienste oder Betreiber öffentlicher Telekommunikationsnetze, die weniger als 50 Mitarbeiter beschäftigen und einen Jahresumsatz oder eine Jahresbilanzsumme von jeweils 10 Millionen Euro oder weniger aufweisen, oder

Nr. 3: eine sonstige natürliche oder juristische Person sowie eine rechtlich unselbstständige Organisationseinheit einer Gebietskörperschaft, die anderen natürlichen oder juristischen Personen entgeltlich Waren oder Dienstleistungen anbieten und die einer der in den Anlagen 1 und 2 bestimmten Einrichtungsarten (z.B. Energie, Transport und Verkehr, Finanz- und Gesundheitswesen, Wasser, Digitale Infrastruktur, Weltraum) zuzuordnen sind und mindestens 50 Personen beschäftigt oder einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro aufweist.

IV. Pflichten der Betreiber von betroffenen Anlagen und Einrichtungen

Die Pflichten der Betreiber der relevanten Anlagen und Einrichtungen werden in Umsetzung des Kapitels IV der NIS2-Richtlinie im dritten Teil, Kapitel 2 BSIG festgelegt. Es bleibt im Wesentlichen bei den Maßnahmen des Risikomanagements (dazu unter III. 1.) und den Meldepflichten (dazu unter III. 2.).

> **SZA-Merkkasten**: Entsprechend der NIS2-Richtlinie unterfallen auch nach dem NIS2UmsG alle Anlagen-/ Einrichtungsbetreiber grundsätzlich denselben Verpflichtungen.

1. Maßnahmen des Risikomanagements

Die Risikomanagementmaßnahmen sind detailliert in § 30 BSIG geregelt. Allerdings wird in der Intensität der jeweiligen Maßnahme aus Gründen der Verhältnismäßigkeit zwischen den Anlagen-/Einrichtungskategorien differenziert. In Abs. 1 werden die Anforderungen an die besonders wichtigen und wichtigen Einrichtungen noch sehr offen formuliert, jedoch sodann durch Abs. 2 entsprechend präzisiert. Danach müssen die Maßnahmen auf einem gefahrenübergreifenden Ansatz beruhen, der zahlreiche Mindestanforderungen erfüllt wie:

Nr. 1: Konzepte in Bezug auf die Risikoanalyse und Sicherheit in der Informationstechnik,

Nr. 2: Bewältigung von Sicherheitsvorfällen,

Nr. 3: Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement,

Nr. 4: Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zu ihren unmittelbaren Anbietern oder Diensteanbietern,

Nr. 5: Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen,

Nr. 6: Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik,

Nr. 7: grundlegende Verfahren im Bereich der Cyberhygiene, Schulungen und Sensibilisierungsmaßnahmen im Bereich der Sicherheit in der Informationstechnik,

Nr. 8: Konzepte und Verfahren für den Einsatz von kryptografischen Verfahren,

Nr. 9: Erstellung von Konzepten für die Sicherheit des Personals, die Zugriffskontrolle und die Verwaltung von IKT-Systemen, -Produkten und -Prozessen,

Nr. 10: Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

2. Meldepflichten

Die Meldepflichten der Anlagen und Einrichtungen ergeben sich aus § 32 BSIG. Danach müssen besonders wichtige und wichtige Einrichtungen im Falle eines erheblichen Sicherheitsvorfalles das dreistufige Meldesystem der NIS2-Richlinie - in Form der Frühwarnung, offiziellen Meldung und Berichterstattung - einhalten.

Ein Sicherheitsvorfall ist ein Ereignis, das die Verfügbarkeit, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über informationstechnische Systeme, Komponenten und Prozesse angeboten werden oder zugänglich sind, beeinträchtigt (vgl. § 2 Nr. 40 BSIG).

Erheblich ist der Sicherheitsvorfall, wenn er nach § 2 Nr. 11 BSIG

a) schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann; oder
b) andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann.

Jedoch soll der bürokratische Aufwand für die Einrichtungen im Rahmen des Umsetzungsspielraums minimiert werden, indem die Übermittlung an das BSI über eine von diesem im Einvernehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe nach Anhörung der betroffenen Betreiber und Wirtschaftsverbände eingerichtete Meldemöglichkeit erfolgt (§ 32 Abs. 4 BSIG).

3. Weitere Informationspflichten

Entsprechend Art. 23 Abs. 1 S. 2 der NIS2-Richtlinie kann das BSI nach § 35 Abs. 1 BSIG die Betreiber wichtiger und besonders wichtiger Einrichtungen verpflichten, die Empfänger der Dienste der Einrichtung unverzüglich zu benachrichtigen, sofern der erhebliche Sicherheitsvorfall die Erbringung des jeweiligen Dienstes beeinträchtigen kann. Allerdings kann die Mitteilung zur vereinfachten Umsetzung auch im Internet veröffentlicht werden.

4. Weitere Pflichten

Darüber hinaus regelt das NIS2UmsG auch weitere einrichtungsspezifische Pflichten, wie etwa:

a. Registrierungspflichten

Nach § 33 BSIG besteht künftig eine Registrierungspflicht für die besonders wichtigen und wichtigen Einrichtungen sowie für Domain-Name-Registry-Diensteanbieter. Die erforderlichen Daten sind an das BSI zu übermitteln. Wird dieser Pflicht nicht nachgegangen, so kann das BSI die Registrierung auch selbst vornehmen (vgl. § 33 Abs. 3 BSIG). Für Betreiber kritischer Anlagen gelten nach § 33 Abs. 2 BSIG strengere Pflichten. Zudem ist in § 34 BSIG eine besondere Registrierungspflicht für bestimmte Einrichtungsarten normiert.

Einrichtungen, die der Registrierungspflicht unterliegen, müssen einen zweistufigen Registrierungs-

prozess durchlaufen.[4] Das BSI empfiehlt, den betreffenden Account bis spätestens zum Jahresende 2025 anzulegen, um sich im zweiten Schritt ab Anfang 2026 beim u.a. für die NIS-2-Richtlinie neu entwickelten BSI-Portal zu registrieren. Dieses soll am 6. Januar 2026 freigeschaltet werden und als Meldestelle für erhebliche Sicherheitsvorfälle dienen.

b. Umsetzungs-, Überwachungs- und Schulungspflichten für Geschäftsleitung

Nach § 38 Abs. 1 BSIG sind die Geschäftsleitungen besonders wichtiger und wichtiger Einrichtungen verpflichtet, die von diesen Einrichtungen nach § 30 BSIG zu ergreifenden Risikomanagementmaßnahmen umzusetzen und ihre Umsetzung zu überwachen. Die Geschäftsleiter haften nach § 38 Abs. 2 BSIG für den bei der Einrichtung durch eine Verletzung der nach Abs. 1 bestehenden Pflicht entstandenen Schaden, entweder gemäß bestehenden allgemeinen gesellschaftsrechtlichen Grundsätzen (z.B. § 93 Abs. 2 AktG) oder in Ermangelung bestehender Haftungsbestimmungen nach dem BSIG.

> **SZA-Merkkasten:** § 38 Abs. 1 BSIG begründet Pflichten, deren Verletzung nach den allgemeinen Grundsätzen des Gesellschaftsrechts oder in Ermangelung solcher Haftungsbestimmungen gemäß § 38 Abs. 2 BSIG zu einer sog. Managerhaftung führen kann.

c. Zusätzliche Anforderungen an Betreiber kritischer Anlagen

Nach § 31 BSIG bestehen zusätzliche Anforderungen an Betreiber kritischer Anlagen. Insbesondere sind diese verpflichtet, für ihre informationstechnischen Systeme, Komponenten und Prozesse Systeme zur Angriffserkennung einzusetzen, die geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten (§ 31 Abs. 2 BSIG). Dieser Einsatz ist wiederum von der Nachweispflicht nach § 39 BSIG erfasst.

V. Durchsetzungsmaßnahmen

1. Etablierung eines „CISO Bund“

Gemäß § 48 BSIG soll der Koordinator der Bundesregierung für Informationssicherheit das operative Informationssicherheitsmanagement des Bundes koordinieren und die Ressorts bei der Umsetzung der Vorgaben für das Informationssicherheitsmanagement unterstützen.

2. Warnungen

Die Möglichkeiten bezüglich der Aussprache von Warnungen durch das BSI sind in § 13 Abs. 1 BSIG geregelt und umfassen:

a) Warnungen vor Schwachstellen und anderen Sicherheitsrisiken in informationstechnischen Produkten und Diensten,
b) Warnungen vor Schadprogrammen,
c) Warnungen bei einem Verlust oder einem unerlaubten Zugriff auf Daten,
d) Informationen über sicherheitsrelevante IT-Eigenschaften von Produkten und
e) Informationen über Verstöße besonders wichtiger Einrichtungen oder wichtiger Einrichtungen gegen die Pflichten aus dem BSIG.

3. Zertifizierungen

Nach § 52 Abs. 2 BSIG kann beim BSI für bestimmte Produkte oder Leistungen eine Sicherheits- oder Personenzertifizierung oder eine Zertifizierung als IT-Sicherheitsdienstleister beantragt werden.

4. Freiwilliges IT-Sicherheitskennzeichen

Das BSI führt zur Information von Verbrauchern über die IT-Sicherheit von Produkten bestimmter vom

[4] Siehe hierzu näher unter https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2025/251205_NIS-2-Umsetzungsgesetz_in_Kraft.html.

Bundesamt festgelegter Produktkategorien ein einheitliches IT-Sicherheitskennzeichen ein (§ 55 Abs. 1 BSIG). Dieses besteht aus einer Herstellererklärung und einer Sicherheitsinformation (vgl. die Legaldefinitionen in § 55 Abs. 2 BSIG). Es trifft indes keine Aussage über die Datenschutzkonformität eines Produktes.

5. Verhängung von Geldbußen und Zwangsgeldern

Sofern die Verletzung einer der oben genannten Pflichten eine Ordnungswidrigkeit darstellt (vgl. Katalog in § 65 Abs. 1-4 BSIG), kann dafür gemäß § 65 Abs. 5 eine Geldbuße verhängt werden. In den Abs. 6 und 7 findet mit Blick auf die Höhe der Geldbuße eine Differenzierung anhand der Einrichtungskategorien statt.

B. Cyber Resilience Act

I. Überblick

Der Cyber Resilience Act vereinheitlicht innerhalb der EU die Regeln zur Cybersicherheit von Produkten mit digitalen Elementen. Das Ziel soll dabei sein, EU-weit vertrauenswürdige und zuverlässige digitale Dienste zu garantieren. Als Verordnung gilt der CRA unmittelbar und bedarf keines nationalen Umsetzungsgesetzes wie bei der NIS2-Richtlinie. Es ist jedoch eine Übergangsfrist vorgesehen, damit die Marktteilnehmer genügend Zeit haben, sich auf die neuen Anforderungen einzustellen und vorzubereiten. Die Umsetzung des CRA erfolgt in verschiedenen Etappen[5] von Ende 2024 bis Ende 2027:

- **11. Juni 2026:** Die Vorschriften über die Notifizierung von Konformitätsbewertungsstellen (KBS) finden Anwendung.

- **11. September 2026:** Die Hersteller von vernetzten Produkten unterliegen der Meldepflicht für aktiv ausgenutzte Schwachstellen und Sicherheitsvorfälle.

- **11. Dezember 2027:** Alle CRA-Anforderungen gelten, einschließlich der Einhaltung der grundlegenden Cybersicherheitsanforderungen vor dem Inverkehrbringen eines Produkts, der Behandlung von Schwachstellen während des gesamten Lebenszyklus des Produkts und der Transparenz gegenüber den Nutzern.

II. Anwendungsbereich

Erfasst werden mit wenigen Ausnahmen alle Produkte mit digitalen Elementen, die auf dem EU-Markt bereitgestellt werden und deren bestimmungsgemäßer Zweck oder vernünftigerweise vorhersehbare Verwendung eine Daten-verbindung mit einem Gerät oder Netz einschließt (Art. 2 CRA). „Produkte" können dabei sowohl Hard- als auch Software sein (Art. 3 Nr. 1 CRA).

III. Pflichten der Wirtschaftsakteure

Durch den CRA werden allen Unternehmen entlang der Lieferkette dieser betreffenden Produkte (Hersteller, Einführer, Händler etc.) Pflichten auferlegt. Den Hersteller der betreffenden Produkte treffen dabei die meisten Pflichten (Art. 13 ff. CRA). Er hat primär dafür zu sorgen, dass seine Produkte den in Anhang I Teil I des CRA benannten Anforderungen gerecht werden. Dazu gehören insbesondere

- eine sichere Konfiguration,
- die Möglichkeit von späteren Sicherheitsaktualisierungen,
- der Schutz von unbefugtem Zugriff, Integrität, Datenminimierung etc.

Zu diesem Zweck muss bereits im Vorhinein eine Risikobewertung für den gesamten Lebenszyklus des jeweiligen Produkts stattfinden, die auch in die technische Dokumentation des Produkts aufgenommen werden muss. Auch nach dem Inverkehrbringen ist regelmäßig für mindestens 5 Jahre eine cybersicherheitstechnische Begleitung des Produkts durch den Hersteller vorzunehmen.

[5] https://digital-strategy.ec.europa.eu/de/factpages/cyber-resilience-act-implementation.

Den Hersteller treffen darüber hinaus Informations- und Meldepflichten, um eine erhöhte Transparenz zu schaffen.
Die Erfüllung der Anforderungen muss der Hersteller durch ein Konformitätsbewertungsverfahren nachweisen (Art. 32 CRA). Wie genau das Verfahren im Einzelfall aussieht, bestimmt sich nach der jeweiligen Einstufung des Produkts in eine von mehreren Risikoklassen. Während für unkritische Produkte bereits eine Selbstbeurteilung ausreichen kann, müssen für Produkte mit höherem Risiko teilweise externe Stellen zur Konformitätsbewertung konsultiert werden. Insofern unterscheidet der CRA nach verschiedenen Produktkategorien.

Die sonstigen Verpflichteten (Einführer und Händler) entlang der Lieferkette (Art. 19 ff. CRA) haben v.a. zu überprüfen, dass die Hersteller der von ihnen eingeführten oder gehandelten Produkte (bestimmte) Anforderungen des CRA erfüllen. Im Übrigen haben sie mit den Marktüberwachungsbehörden zu kooperieren.

IV. Verhängung von Geldbußen und Zwangsgeldern

Verstöße gegen den CRA können im Einzelfall mit hohen Bußgeldern (bis zu 15 000 000 EUR oder bis zu 2,5 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres, je nachdem, welcher Betrag höher ist) geahndet werden (Art. 64 CRA).

C. Praxishinweise

Unternehmen sollten kritisch prüfen, ob sie in den (persönlichen) Anwendungsbereich der NIS2-Richtlinie und damit des NIS2UmsG fallen. Ist dies der Fall, sollten umgehend die Anforderungen der NIS2-Richtlinie identifiziert und Maßnahmen zur Erfüllung der Verpflichtungen ermittelt werden.

Aufgrund des erfahrungsgemäß langen Implementierungs-zeitraums von Sicherheitssystemen und -konzepten raten wir betroffenen Unternehmen weiterhin an, unverzüglich mit der Implementierung entsprechender Maßnahmen zu beginnen. Dies ist nicht zuletzt auch mit Blick auf die im NIS2UmsG etablierten Geschäftsleitungspflichten und der damit verbundenen Managerhaftung dringend geboten.

Gerne unterstützen wir Sie bei der Implementierung eines der Anforderungen der NIS2-Richtlinie entsprechenden Cybersicherheitsrahmens.

Die Empfehlung einer möglichst frühen Implementierung entsprechender Maßnahmen gilt auch in Bezug auf die Regelungen des CRA, auch wenn die Anforderungen der Verordnung teilweise erst ab Ende 2027 gelten.

Im Übrigen bleibt die legislative Entwicklung auf EU- und nationaler Ebene abzuwarten. Nur drei Jahre nach Erlass der NIS-2-Richtlinie schlug die Kommission mit ihrem Digital Omnibus-Entwurf vom 19. November 2025 bereits Änderungen der NIS2-Richtlinie vor. Diese betreffen die Etablierung eines „single entry points“ zur Meldung von Sicherheitsvorfällen gem. Art. 23 NIS2-Richtlinie. Damit ist eine von der EU bereitzustellende Schnittstelle zwischen den Unternehmen und den Aufsichtsbehörden gemeint, die die Unternehmen grundsätzlich zur Meldung von Sicherheitsvorfällen verwenden müssen.

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
Partner
Gewerblicher Rechtsschutz

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

Dr. Marc Löbbe
Partner
Gesellschaftsrecht / M&A / Compliance

T +49 69 976 96 01 201
E Marc.Loebbe@sza.de

Dr. Steffen Henn
Counsel
Gewerblicher Rechtsschutz

T +49 621 4257 386
E Steffen.Henn@sza.de

Dr. Anke Hofmann
Senior Associate
Gewerblicher Rechtsschutz

T +49 621 4257 222
E Anke.Hofmann@sza.de

Serpil Dilbaz, LL.B.
Associate
Gewerblicher Rechtsschutz

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