orka Newsletter | Datenschutz, IT & Outsourcing

Neuer Gesetzesentwurf zur Umsetzung der NIS-2-Richtlinie veröffentlicht

Die Umsetzung der NIS-2-Richtlinie (RL (EU) 2022/2555) in deutsches Recht schreitet voran. Das Bundesministerium des Innern und für Heimat (BMI) der neuen Bundesregierung hat einen neuen Referentenentwurf eines Gesetzes zur **Umsetzung der europäischen NIS-2-Richtlinie** veröffentlicht (Datum 26.05.2025).

Eigentlich hätte die NIS-2-Richtlinie, deren Ziel die **Einführung von EU-weiten Mindeststandards im Bereich der Cybersicherheit** ist, bereits seit dem 17. Oktober 2024 in deutsches Recht umgesetzt worden sein müssen. Aufgrund der Neuwahlen zum Deutschen Bundestag und des sog. Diskontinuitätsprinzips konnte das bereits fortgeschrittene Gesetzgebungsverfahren bezüglich des Gesetzesentwurfs, der noch von der Ampel-Regierung stammte, nicht fortgeführt werden. Daher leitete die EU-Kommission u.a. gegen Deutschland ein Vertragsverletzungsverfahren ein.

Der jetzt veröffentlichte Gesetzesentwurf beruht auf dem letzten Entwurf der vorherigen Ampel-Regierung und enthält nur wenige Änderungen im Bereich der Vorschriften für Unternehmen. Wir informieren Sie über den aktuellen Stand der NIS-2-Umsetzung.

Weitere Informationen zu unseren Veröffentlichungen und Webinaren auch rund um das Thema „*IT-Sicherheit / NIS-2*“ erhalten Sie hier.

Betroffene Unternehmen

Entsprechend der Vorgaben der europäischen NIS-2-Richtlinie sorgen die neuen gesetzlichen IT-Sicherheitsvorschriften für einen erweiterten Rechtsrahmen, insbesondere durch eine **erhebliche Ausweitung der verpflichteten Unternehmen**, die Festlegung neuer Mindestsicherheitsanforderungen sowie erweiterte Meldepflichten bei Sicherheitsvorfällen.

Bislang war der Anwendungsbereich des BSI-Gesetzes grundsätzlich auf Betreiber kritischer Infrastrukturen (**sog. KRITIS-Betreiber**) fokussiert, die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind. Der **Anwendungsbereich** der neuen gesetzlichen Vorschriften wird zukünftig erheblich ausgeweitet und **erfasst eine Vielzahl von Unternehmen**.

KRITIS-Betreiber	Gesundheit	Öffentliche Verwaltung	Lebensmittel
Energie	Wasser	Post- / Kurierdienste	Verarbeitendes Gewerbe
Transport / Verkehr	IKT-Dienste	Abfallwirtschaft	Forschung
Finanzen / Versicherungen	Weltraum	Chemie	Digitale Dienste

Der Kreis der verpflichteten Unternehmen erfasst grundsätzlich drei Bereiche:

(1) Als „**besonders wichtige Einrichtungen**“ gelten insbesondere Unternehmen aus bestimmten Sektoren (**s. Grafik: rot markierte Sektoren**), die *(i)* mindestens 250 Mitarbeiter beschäftigen oder *(ii)* einen Jahresumsatz von über 50 Mio. Euro und zudem eine Jahresbilanzsumme von über 43 Mio. Euro aufweisen.

(2) Als „**wichtige Einrichtungen**“ gelten insbesondere Unternehmen aus bestimmten Sektoren (**s. Grafik: rot und blau markierte Sektoren**), die *(i)* mindestens 50 Mitarbeiter beschäftigen oder *(ii)* einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Mio. Euro aufweisen.

(3) Daneben besteht – vergleichbar zu den bisherigen KRITIS-Betreibern – die Kategorie der „**Betreiber kritischer Anlagen**“, d.h. insbesondere Unternehmen, die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss auf eine oder mehrere kritische Anlagen ausübt.

Die konkret betroffenen Anlagenarten sowie die maßgeblichen Schwellenwerte für die Qualifikation als „Kritische Anlage“ werden auch zukünftig durch die **KRITIS-Verordnung** festgelegt. Bislang ist noch nicht bekannt ist, ob die Schwellenwerte der KRITIS-Verordnung verändert werden. Im Hinblick auf die KRITIS-Verordnung sieht der aktuelle Gesetzesentwurf zwei wesentliche Änderungen vor:

- Der **Begriff „*Betreiber*“** soll aus der KRITIS-Verordnung gestrichen werden.
- Im Sektor „*Energie*“ ist die **neue Anlagenkategorie „*Digitaler Energiedienst*“** vorgesehen.

Für **Unternehmen aus dem Sektor „*Energie*“** sind die geplanten Änderungen des Energiewirtschaftsgesetzes (EnWG) relevant. Diesbezüglich sieht der Gesetzesentwurf vor, dass die bisherigen IT-Sicherheitsanforderungen in § 11 Abs. 1a – 1g EnWG durch einen neuen § 5c EnWG ersetzt werden, der sich stärker

den Vorgaben der NIS-2-Richtline orientieren soll. Zu den IT-Sicherheitsanforderungen im Sektor „*Energie*“ werden wir einen gesonderten Newsletter veröffentlichen.

Risikomanagement

Im Fokus der neuen gesetzlichen Vorschriften steht die weitreichende **Pflicht zur Ergreifung von Risikomanagementmaßnahmen**. Betroffene Unternehmen werden verpflichtet, geeignete technische und organisatorische Maßnahmen zu ergreifen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten. Die ergriffenen Maßnahmen müssen dokumentiert werden, um eine Nachweisbarkeit zu ermöglichen.

Die zu ergreifenden technischen und organisatorischen Maßnahmen sollen den jeweiligen **Stand der Technik** einhalten, die einschlägigen europäischen und internationalen Normen berücksichtigen und müssen auf einem **gefahrenübergreifenden Ansatz** beruhen. Unternehmen werden insoweit verpflichtet, die relevanten Risiken kontinuierlich zu überwachen und die ergriffenen Maßnahmen fortlaufend anzupassen.

Betreiber kritischer Anlagen müssen **besonders weitreichende Risikomanagementmaßnahmen** ergreifen. Für sie gelten auch aufwändigere technische und organisatorische Maßnahmen noch als verhältnismäßig und zumutbar.

Registrierungspflichten

Betroffene Unternehmen sind zur **Registrierung** verpflichtet. In zeitlicher Hinsicht muss die Registrierung **spätestens drei Monate**, nachdem ein Unternehmen erstmalig oder erneut in den Anwendungsbereich der neuen gesetzlichen Vorschriften fällt, vorgenommen werden. Die im Rahmen der Registrierung mitgeteilten Informationen müssen **kontinuierlich aktualisiert** werden, sofern sich die relevanten Aspekte ändern.

Anbieter bestimmter Dienste, u.a. Anbieter von Cloud-Computing-Diensten und Rechenzentrumsdiensten, Managed Service Provider oder Anbieter von Online-Marktplätzen, treffen darüber hinaus besondere Registrierungspflichten.

Verstöße gegen die Registrierungs- und Mitteilungspflichten sind bußgeldbewehrt und können mit **Geldbußen in Höhe von bis zu 500.000 Euro** geahndet werden.

Meldepflichten

Bislang sah das BSI-Gesetz ein einstufiges **Meldeverfahren bei Störungen** relevanter Einrichtungen und Systeme vor. Die bislang einstufige Meldepflicht wird durch ein **dreistufiges Melderegime** ersetzt.

Damit soll den Interessen an einer schnellen sowie gleichermaßen detaillierten Meldung von Sicherheitsvorfällen Rechnung getragen werden.

(1) Auf der **ersten Stufe** sind betroffene Unternehmen, unverzüglich, spätestens jedoch **innerhalb von 24 Stunden** nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall, zu einer frühen Erstmeldung verpflichtet.
In der frühen Erstmeldung muss angegeben werden, ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte.
(2) Auf der **zweiten Stufe** müssen betroffene Unternehmen **innerhalb von 72 Stunden** nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall eine ausführlichere Meldung einschließlich einer Risikobewertung des Sicherheitsvorfalls an die zuständige Behörde richten.
(3) **Spätestens einen Monat** nach Übermittlung dieser Meldung muss sodann auf der **dritten Stufe** eine ausführliche Abschlussmeldung zu dem Sicherheitsvorfall erfolgen.

Betroffenen Unternehmen ist zu empfehlen, zur Umsetzung der Meldepflichten **Notfallprozesse zu etablieren**, um die Einhaltung der sehr kurzen Fristen gewährleisten zu können. Dies ist nicht zuletzt relevant, da Verstöße gegen die gesetzlichen Meldepflichten mit **Geldbußen in Höhe von bis zu 10 Mio. Euro bzw. 2 Prozent des globalen Jahresumsatzes** geahndet werden können.

Parallel zu den Meldepflichten kann das BSI die betroffenen Unternehmen im Falle von erheblichen Sicherheitsvorfällen anweisen, **die Empfänger ihrer Dienste** (z.B. Kunden) unverzüglich über den Sicherheitsvorfall **zu unterrichten**, zum Beispiel durch Veröffentlichung von Informationen auf einer Internetseite.

Einrichtungen aus bestimmten Sektoren (Finanz- und Versicherungswesen, Informationstechnik und Telekommunikation, Verwaltung von IKT-Diensten und Digitale Dienste) müssen den potenziell von einer erheblichen Cyberbedrohung betroffenen Empfängern ihrer Dienste sowie dem BSI zudem unverzüglich alle Maßnahmen mitteilen, die diese Empfänger als Reaktion auf diese Bedrohung ergreifen können, sofern die Empfänger ein überwiegendes Interesse an solchen Informationen haben.

Governancepflichten der Geschäftsleitung

Eine besonders relevante Neuheit im Vergleich zur bisherigen Rechtslage sind **weitreichende Pflichten und damit einhergehende Haftungsrisiken für die Geschäftsleitungen** betroffener Unternehmen. Der Gesetzesentwurf sieht nämlich weitreichende Umsetzungs-,

Überwachungs- und Schulungspflichten für die Geschäftsleitungen betroffener Unternehmen vor.

Die Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen werden insbesondere verpflichtet, die von ihrer Einrichtung ergriffenen **Risikomanagementmaßnahmen umzusetzen und ihre Umsetzung zu überwachen**.

Zudem sieht das Gesetz vor, dass die Geschäftsleitungen betroffener Unternehmen **regelmäßig (mind. alle 3 Jahre) persönlich an Schulungen teilnehmen** müssen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Risikomanagementpraktiken im Bereich der IT-Sicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben.

Sofern einem Unternehmen ein Schaden entsteht, weil die Geschäftsleitung ihren Pflichten nicht hinreichend nachgekommen ist, kann sich unter Umständen ein **Haftungsanspruch der Gesellschaft gegenüber der Geschäftsleitung** ergeben. Unsicher ist aktuell noch, ob ein Verzicht des Unternehmens auf Ersatzansprüche gegen die Geschäftsleitung wirksam möglich sein wird oder nicht. Unternehmen könnten unter Umständen gezwungen sein, die ihnen gegen die Geschäftsleitung zustehenden Ersatzansprüche auch tatsächlich geltend zu machen.

Unsere Empfehlung

Die europäische NIS-2-Richtlinie und das deutsche Umsetzungsgesetz sorgen für eine **erhebliche Erweiterung des Anwendungsbereichs der verpflichteten Unternehmen**. In der Folge müssen viele Unternehmen erstmalig die strengen gesetzlichen Vorschriften zur IT-Sicherheit beachten.

Zugleich werden die **Pflichten betroffener Unternehmen ausgeweitet und inhaltlich verschärft**, nicht zuletzt durch die unmittelbaren Verpflichtungen der Geschäftsleitungen und das damit einhergehende Haftungsrisiko.

Die Umsetzung der gesetzlichen Anforderungen geht für betroffene Unternehmen sowohl in rechtlicher als auch in technischer und organisatorischer Hinsicht mit einem erheblichen Aufwand einher. **Daher sollten betroffene Unternehmen keine Zeit verlieren und bereits jetzt mit der Umsetzung beginnen.**

Zwar hat der deutsche Gesetzgeber **zum aktuellen Zeitpunkt im Juni 2025** noch kein Umsetzungsgesetz final beschlossen und verabschiedet. Unmittelbare Pflichten ergeben sich für Unternehmen in Deutschland erst mit dem Inkrafttreten eines deutschen Umsetzungsgesetzes. Der aktuelle Gesetzesentwurf und die verbindliche Fassung der europäischen NIS-2-Richtlinie können jedoch als Grundlage für die Umsetzung der erforderlichen Maßnahmen dienen.

Ihre Ansprechpartner

Dr. Ulla Kelp, LL.M.
Rechtsanwältin, Partnerin

T +49 211 600 35-176
ulla.kelp@orka.law

Dr. Philipp Mels
Rechtsanwalt, Partner

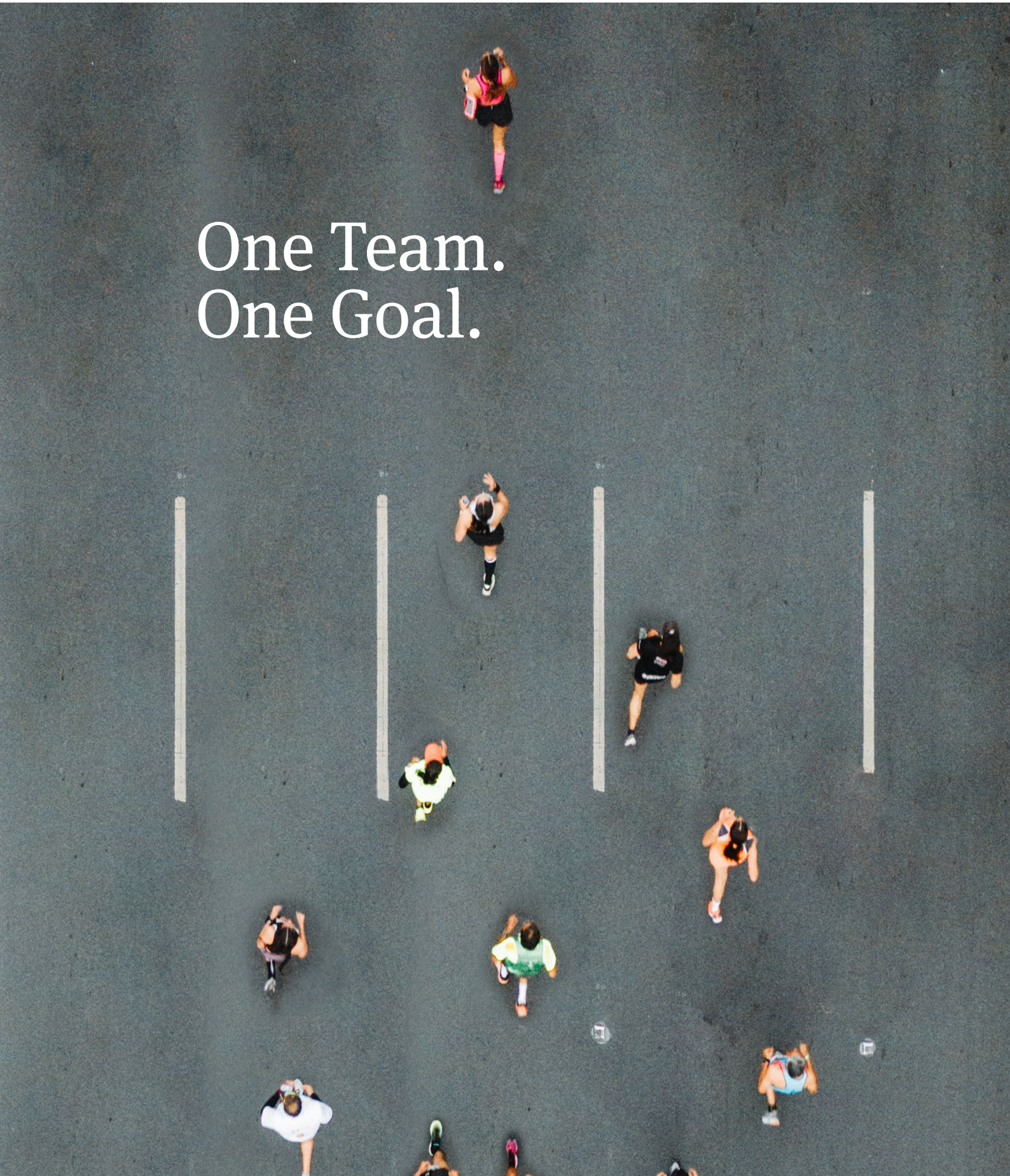
T +49 211 600 35-180
philipp.mels@orka.law

Dr. Michael Grobe-Einsler
Rechtsanwalt, Salary Partner

T +49 211 600 35-450
michael.grobe-einsler@orka.law

Felix Meurer
Rechtsanwalt, Salary Partner

T +49 30 50 93 20-117
felix.meurer@orka.law


One Team.
One Goal.