



One Team.
One Goal.

IP / IT / Datenrecht

Neue Pflichten für Unternehmen im Bereich der IT-Sicherheit

Das Bundesministerium des Innern und für Heimat (BMI) hat am 7. Mai 2024 einen neuen Referentenentwurf eines Gesetzes zur **Umsetzung der europäischen NIS-2-Richtlinie** veröffentlicht. Das sog. „NIS-2-Umsetzungs- und Cyber-sicherheitsstärkungsgesetz“ **kurz: „NIS2UmsuCG“** dient der Umsetzung der europäischen NIS-2-Richtlinie in das nationale Recht und sorgt für eine erhebliche Erweiterung des Adressatenkreises sowie weitreichende Pflichten im Bereich der IT-Sicherheit.

Die europäische NIS-2-Richtlinie (Richtlinie (EU) 2022/2555) ist bereits im Januar 2023 in Kraft getreten und muss von den EU-Mitgliedstaaten **bis zum 17. Oktober 2024** in nationales Recht umgesetzt werden. Der deutsche Gesetzgeber hatte

bereits im Frühjahr 2023 einen ersten Gesetzesentwurf veröffentlicht, dieser wurde sodann jedoch mehrfach sukzessive verändert. Infolgedessen wurde bislang kein finaler Gesetzesentwurf in den Deutschen Bundestag eingebracht.

Das **Ziel der neuen gesetzlichen Vorschriften** ist die Einführung von EU-weiten Mindeststandards für Unternehmen, wodurch ein hohes gemeinsames Cybersicherheitsniveau sichergestellt werden soll. Die Wirtschaft als auch staatliche Institutionen sollen vor Schäden durch Cyberangriffe wie beispielsweise Ransomware-Attacken oder Supply Chain-Angriffe, die infolge der zunehmenden Digitalisierung und Vernetzung in ihrer Intensität und Reichweite stetig zunehmen, geschützt werden.

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.

Betroffene Unternehmen

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 dementsprechend **erheblich ausgeweitet** und erfasst eine Vielzahl von Unternehmen.

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 sog. **Betreiber kritischer Anlagen**, d.h. insbesondere Unternehmen, die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände einen bestimmenden Einfluss auf eine oder mehrere kritische Anlagen ausüben. In Bezug auf die „Kritischen Anlagen“ benennt der Gesetzesentwurf die Sektoren Energie, Transport und Verkehr, Finanz- und Versicherungswesen, Gesundheitswesen, Wasser, Ernährung, Informationstechnik und Telekommunikation, Weltraum oder Siedlungsabfallentsorgung.

Die konkret betroffenen Anlagenarten sowie die maßgeblichen Schwellenwerte für die Qualifikation als „Kritische Anlage“ werden – parallel zur bisherigen „KRITIS-Verordnung“ – durch eine Rechtsverordnung festgelegt. Bis Mitte Mai 2024 hat die Bundesregierung eine solche Rechtsverordnung noch nicht veröffentlicht.

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

Grafik: Übersicht NIS-2 Sektoren



Risikomanagement

Im Fokus der neuen gesetzlichen Vorschriften steht die reichweitende **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. Die betroffenen Unternehmen sind verpflichtet, bis zum 17. Januar 2025 weitergehende Angaben an die zuständigen Behörden mitzuteilen.

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 infolge der neuen gesetzlichen Vorschriften durch ein **dreistufiges Melderegime** ersetzt.

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

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.

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. **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, **Prozesse** bezüglich der erforderlichen Maßnahmen zur **Umsetzung der Meldepflichten** 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 Billigungs-, 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 zu billigen und ihre Umsetzung zu überwachen**.

Zudem sieht das Gesetz vor, dass die Geschäftsleitungen betroffener Unternehmen **regelmäßig 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 gesetzlichen Pflichten nicht hinreichend nachgekommen ist, ist ein **Verzicht des Unternehmens auf Ersatzansprüche gegen die Geschäftsleitung unwirksam**. Unternehmen könnten daher regelmäßig gezwungen sein, die ihnen gegen die Geschäftsleitung zustehenden Ersatzansprüche auch tatsächlich geltend zu machen.

Gleichermaßen sollen Vergleichsvereinbarungen über entsprechende Ersatzansprüche unwirksam sein, sofern ein Vergleich in einem groben Missverhältnis zu der bestehenden Rechtsunsicherheit über das jeweilige Rechtsverhältnis steht.

Eine **sehr enge Ausnahme** bezüglich der Unwirksamkeit solcher Vergleiche oder Verzichte sieht das Gesetz nur für die Fälle vor, dass der Ersatzpflichtige zahlungsunfähig ist und sich zur Abwendung des Insolvenzverfahrens mit seinen

Gläubigern vergleicht bzw. wenn die Ersatzpflicht in einem Insolvenzplan geregelt wird.

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.

Zwar existiert zum aktuellen Zeitpunkt Mitte Mai 2024 noch kein finaler Gesetzesentwurf in Deutschland. Unmittelbare Pflichten ergeben sich für Unternehmen in Deutschland erst mit dem Inkrafttreten eines deutschen Umsetzungsgesetzes. Der Referentenentwurf vom 7. Mai 2024 und die verbindliche Fassung der europäischen NIS-2-Richtlinie können jedoch als **Grundlage für die Umsetzung** der erforderlichen Maßnahmen dienen.

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**.

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, Senior Associate

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



Rafael Wolter, Lic. en droit (LL.B.)
Rechtsanwalt, Associate

T +49 211 600 35-183
rafael.wolter@orka.law



Prof. Dr. Michael Bohne
Of Counsel

T +49 211 600 35-174
michael.bohne@orka.law

One Team.
One Goal.

