Autoren: **Dr. Thomas Willaschek** & **Sebo-Franz Krubally**
Luther Rechtsanwaltsgesellschaft mbH | Berlin
✆ 030 – 52133 24925|✉ thomas.willaschek@luther-lawfirm.com

# NIS2-Richtlinie | Relevanz und Folgen der NIS2-Gesetzgebung für MVZ und Großpraxen

## WORUM GEHT'S?

*Dieser Beitrag beleuchtet dem aktuellen Stand des Gesetzgebungsverfahrens zur Überführung der Vorgaben der zweiten EU-Richtline zur Netzwerk- und Informationssicherheit (NIS-2-Richtlinie) in deutsches Recht. Er soll der Geschäftsführung von größeren bzw. umsatzstarken MVZ, BAG und sonstige (Groß-)Praxen erste Orientierung über die Relevanz und Folgen dieses Umsetzungsaktes bieten.*

## AKTUELLER STAND

Die Europäische Union (EU) hat im Dezember 2022 die NIS-2-Richtlinie verabschiedet. Hiermit wurden die durch die Weiterentwicklungen in Technik und Wirtschaft gestiegenen Anforderungen an die Cybersicherheit von Unternehmen in der EU rechtlich fixiert. Die EU-Vorgaben sollen mit dem sog. NIS-2-Umsetzungs und Cybersicherheitsstärkungsgesetz (**NIS-2-UmsuCG**) in deutsches Recht überführt werden. Das NIS-2-UmsuCG sieht unter anderem die Überarbeitung des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (**BSIG**) vor.

Ziel des NIS-2-UmsuCG ist es, die Resilienz von Unternehmen im Bereich Cybersicherheit zu stärken. Der Gesetzesentwurf nennt hierbei als typische, zu verhütende Bedrohungslage unter anderem Ransomware-Angriffe auf Server medizinischer Einrichtungen, die die lückenlose ambulante Versorgung beeinträchtigen können (BT-Drs. 20/13184, S.3).

Unter die mit dem NIS-2-UmsuCG angepasste Rechtslage werden in Deutschland künftig ca. 30.000 Unternehmen fallen. **Folgen hat dies unter anderem auch für Einheiten in der ambulanten ärztlichen Versorgung**, insbesondere größere Medizinische Versorgungszentren (MVZ) und Berufsausübungsgemeinschaften (BAG), die teilweise erstmals umfassend zur Cybersicherheit verpflichtet sein werden.

Die EU-Gesetzgeber verpflichtete die Mitgliedsstaaten dazu, die Vorgaben der NIS-2-Richtlinie bis zum 17. Oktober 2024 in nationales Recht zu überführen. Aus Sicht des deutschen Gesetzgebers ist diese Frist fruchtlos abgelaufen.

Erst am 24. Juli 2024 hat das Bundeskabinett den Entwurf des NIS-2-UmsuCG beschlossen. Der Bundestag hat sich in der Folge erstmals am 11. Oktober 2024 mit dem Gesetzesentwurf befasst und die Vorlage anschließend zur weiteren Beratung an den Innenausschuss weitergleitet. In der öffentlichen Anhörung am 4. November 2024 äußerten die von den Fraktionen entsandten Experten erhebliche Kritik am Entwurf. Bemängelt wurde neben den zu weitreichenden Ausnahmeregelungen für die (untergeordnete) Verwaltung und Forschung auch, dass Unternehmen selbst herausfinden müssen, ob sie eine vom künftigen BSIG betroffene Einrichtung sind. Der Entwurf sieht nämlich gerade nicht verbindlich vor, dass das BSI als Aufsichtsbehörde die Unternehmen dahingehend informiert.

Nachdem die Umsetzungsfrist zum 17. Oktober 2024 versäumt wurde, rechnete man zunächst mit Inkrafttreten des NIS-2-UmsuCG zum Frühjahr 2025. Durch den Bruch der Ampel-Koalition erscheint auch dieses Umsetzungsdatum nun ungewiss. Der Bundeskanzler hat am 16. Dezember 2024 die Vertrauensfrage gestellt; Folge sind die für 23. Februar 2025 angesetzten, vorgezogenen Neuwahlen.

Vom aktuellen Bundestag sollen Gesetzgebungsverfahren, die keinen Aufschub mehr dulden, abgeschlossen werden. Das NIS2UmsuCG wurde in diesem Zusammenhang bisher nicht ausdrücklich genannt. Allerdings scheint die baldige Umsetzung der EU-Vorgaben weiterhin fraktionsübergreifend für

dringlich gehalten zu werden; dies nicht zuletzt auch vor dem steigenden Risiko eines Vertragsverletzungsverfahrens bei weiteren substanziellen Verzögerungen. Eventuell wird der Gesetzesentwurf im aktuellen Bundestag in die zweite und dritte Lesung gehen und verabschiedet. Andernfalls wird absehbar dies früh in der kommenden Legislaturperiode erfolgen.

Sicher ist jedenfalls, dass die Verpflichtung deutscher Unternehmen nach den NIS-2-Vorgaben kommen wird. Potenziell betroffene Unternehmen und damit auch größere ambulante Einheiten sollten sich daher möglichst bald genauer mit den zu erwartenden gesetzgeberischen Vorgaben und dem Stand der eigenen Cybersicherheit im Unternehmen auseinandersetzen.

## BETROFFENHEIT ALS WICHTIGE EINRICHTUNG

Das NIS-2-UmsuCG ist insbesondere für sogenannte
„wichtige Einrichtungen“ im Sinne des BSIG-E relevant.

In seiner derzeitigen Fassung verpflichtet das BISG aktuell nur sogenannte Betreiber kritischer Infrastrukturen zur Erfüllung gesteigerter Anforderungen an die Cybersicherheit. Im Gesundheitssektor sind davon bisher in erster Linie zugelassene Krankenhäuser betroffen, soweit sie die entsprechenden Schwellwerte für eine Einordnung als Kritische Anlage erreichen (mind. 30.000 vollstationäre Fälle/Jahr).

**Das NIS-2-UmsuCG wird den Kreis betroffener Einrichtungen stark ausdehnen.** Künftig sollen nun „besonders wichtige Einrichtungen“ sowie „wichtige Einrichtungen“ verpflichtet werden. Aus Sicht von größeren Praxen – also vor allem MVZ und Berufsausübungsgemeinschaften – ist dabei der Begriff der „wichtigen Einrichtung“ von besonderem Interesse. Künftig fallen darunter gemäß des im NIS-2-UmsuCG enthaltenen § 28 Abs. Abs. 2 Nr. 3 BSIG-E jedenfalls Einrichtungen die

- mindestens **50 Mitarbeiter** beschäftigen
  **oder**
- einen Jahresumsatz und eine Jahresbilanzsumme von
  jeweils über **10 Millionen Euro** aufweisen.

Von den künftig etwa 30.000 vom NIS-2-UmsuCG betroffenen Unternehmen sollen - nach Schätzung des Regierungskabinetts - voraussichtlich rund 20.900 als wichtige Unternehmen einzuordnen sein (BT-Drs. 20/13184, S.109).

**Nach Einschätzung des BMVZ dürfte** wohl der Großteil der rund 800 MVZ mit zweistelligen Arztzahlen (Stand: Ende 2023) bereits das erste Kriterium erfüllen und somit als wichtige Einrichtung gelten. Gemeinsam mit den nach Angaben des BMVZ rund 230 Berufsausübungsgemeinschaften mit zweistelligen Arztzahlen ist von einer Betroffenheit von rund 1.000 Praxen auszugehen. Soweit die Betroffenheit sich nicht (schon) aus der Mitarbeiterzahl ergibt, dürften künftig zusätzlich auch Praxen mit umsatzstarken Schwerpunkten wie etwa der Radiologie, Nuklearmedizin, Nephrologie und Laboratoriumsmedizin bei Erreichen der Umsatzschwelle und Jahresbilanzsumme von 10 Millionen Euro entsprechend erfasst sein (vgl. BT-Drs. 20/13184, S.197).

Ob ein Unternehmen (künftig) von den neuen Bestimmungen betroffen ist, muss dieses selbst anhand der festgelegten Kriterien prüfen. Der Gesetzentwurf sieht gerade nicht vor, dass das BSI alle betroffenen Unternehmen automatisch prüft und diese anschließend über ihre Betroffenheit informiert.

Um die maßgeblichen Umsätze und Mitarbeiterzahlen zu ermitteln, kann auf die Empfehlungen der Kommission zur „*Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen*“ (2003/361/EG) zurückgegriffen werden, auf die das BSIG-E verweist. Hieraus und aus der Entwurfsbegründung ergibt sich folgendes:

- **Partner- bzw. verbundene Unternehmen**: Partner- bzw. verbundene Unternehmen sind im wesentlichen Unternehmen, die sich durch Beteiligungen oder Verträge beeinflussen können. Die Umsätze und Mitarbeiterzahlen solcher Unternehmen werden im Grunde nur bei (i) gemeinsamer oder voneinander abhängiger sowie von einer Konzernmutter vollständig kontrollierter IT-

Infrastruktur und (ii) soweit sie ebenfalls im Gesundheitssektor tätig sind, (anteilig) mitberücksichtigt.

- **Zugelassene Vertragsärzte/Gesellschafter** werden bei der Berechnung der relevanten Mitarbeiterzahlen berücksichtigt, soweit sie tatsächlich im Unternehmen mitarbeiten.
- **Mitarbeiter in Teilzeit** werden anteilig berücksichtigt.
- **Auszubildende/Weiterbildungsassistenten** werden nicht berücksichtigt
- **Mitarbeiter in Mutterschutz/Elternzeit** werden nicht berücksichtigt.
- **Ausscheidende Mitarbeiter**:
  Mitarbeiter, die während des Geschäftsjahres ausscheiden, werden anteilig berücksichtigt.
- **Freie Mitarbeiter**: Mitarbeiter, die etwa von externen Dienstleistern gestellt werden, werden bei der Berechnung grundsätzlich nicht berücksichtigt. Etwas anderes gilt allerdings, wenn diese Mitarbeiter in einem Unterordnungsverhältnis zum Unternehmen stehen und deshalb Arbeitnehmern gleichgestellt sind (sog. Scheinselbstständige). Umstände, die für eine abhängige Beschäftigung sprechen, können sein: Umfassende Weisungsbefugnisse des Unternehmens, Verwendung der Betriebsmittel des Unternehmens, Tätigkeit ausschließlich für das Unternehmen oder Vertretung des Mitarbeiters bei Abwesenheit durch Arbeitnehmer des Unternehmens.

**Das bedeutet konkret für MVZ und überörtliche Berufsausübungsgemeinschaften (üBAG):**

- **MVZ-Gesellschaft mit mehreren MVZ:**
  Es sind die Umsätze und Mitarbeiterzahlen aller MVZ kumuliert zu betrachten.
- **(Krankenhaus-)Gesellschaft mit Mehrheitsbeteiligungen an mehreren MVZ-Gesellschaften:**
  Entscheidend ist die IT-Infrastruktur. Nur wenn die einzelne MVZ-Gesellschaft beherrschenden Einfluss auf die eigene IT hat, wird sie isoliert betrachtet. Dafür muss sie die Entscheidungen über die Beschaffung, den Betrieb und die Konfiguration eigenverantwortlich treffen können. Dies ist zu verneinen, wenn die IT von der Muttergesellschaft betrieben wird. Bei Betrieb der IT-Infrastruktur durch einen externen Dienstleister kann hingegen vertraglich geregelt werden, dass die MVZ-Gesellschaft bestimmenden Einfluss auf die entsprechenden Prozesse nehmen kann – das führt zur isolierten Betrachtung des MVZ.
- **üBAG:** Es sind sämtliche Mitarbeiter und Umsätze, die an den jeweiligen Standorten tätig sind bzw. generiert werden, zu berücksichtigen.

**Wichtig:**
Holen Sie zur Bewertung komplexerer Strukturen stets Rechtsrat ein.

Zur Erleichterung der Prüfung stellt das BSI Unternehmen ein Online-Tool zur Verfügung (zuletzt abgerufen am 20.11.2024), welches allerdings nur beschränkt weiterhilft. Eine hiermit durchgeführte Prüfung führt außerdem zu keinem rechtsverbindlichen Ergebnis und kann allenfalls zur ersten Orientierung dienen. Im Zweifel ist eine Prüfung unter Einbindung juristischer Expertise unerlässlich; dies etwa, um etwa innerhalb von komplexeren Unternehmensstrukturen die zur Einordnung als „wichtige Einrichtung“ relevante Mitarbeiterzahl zu bestimmen.

## (Geplante) PFLICHTEN

Betroffene Einrichtungen werden durch das NIS-2-UmsuCG in der
Entwurfsfassung (BSIG-E) künftig insbesondere die folgenden Pflichten auferlegt:

- **Registrierungspflicht** (§ 33 Abs. 1 BSIG-E): Betroffene Einrichtungen werden sich – nachdem sie ihre Betroffenheit selbst geprüft haben – beim BSI entsprechend registrieren müssen. Kommt die Einrichtung dieser Pflicht nicht nach, kann das BSI die Registrierung selbst vornehmen (vgl. § 33 Abs. 3 BSIG-E). Entsprechende Nachprüfungen sind z. B. in Form von Stichproben bei nicht registrierten

Unternehmen, etwa auf Grundlagen der Daten aus dem Handelsregister und dem Unternehmensregister des Statistischen Bundesamtes denkbar.

- **Meldepflicht** (§ 32 Abs. 1 BSIG-E): Der Entwurf sieht für den Fall von erheblichen Sicherheitsvorfällen konkrete Meldepflichten vor. Dies unter anderem im Falle von Ereignissen, die die Verfügbarkeit, Integrität oder Vertraulichkeit der vom betroffenen Unternehmen verarbeiteten Daten beeinträchtigen und beim Unternehmen schwerwiegende Betriebsstörungen bzw. finanzielle Verluste oder erhebliche Schäden bei anderen Personen auslösen können (vgl. zur Definitionen § 2 Nr. 11 und Nr. 40 BSIG-E). § 32 Abs. 1 BSIG-E sieht in vor, dass die Pflicht zur Erstmeldung innerhalb von 24 Stunden ab Kenntniserlangung vor. Anschließend hat das Unternehmen 72 h nach der Erstmeldung eine bestätigende oder aktualisierende Meldung nebst erster Risikobewertung abzugeben; daneben sieht kann das BSI das Unternehmen zudem zur Abgabe von Zwischenmeldungen auffordern. Einen Monat nach Übermittlung der bestätigenden Meldung soll das Unternehmen gegenüber dem BSI eine sog. Abschlussmeldung machen müssen.
- **Unterrichtungspflicht** (§ 35 BSIG-E): Das BSI kann im Falle von erheblichen Sicherheitsvorfällen zudem anordnen, dass die voraussichtlich betroffenen Empfänger der Dienste – im Falle von Arztpraxen, die Patienten – von der Einrichtung über den Sicherheitsvorfall informiert werden.
- **Risikomanagementmaßnahmen** (§ 35 BSIG-E): Der BISG-E sieht auch die Verpflichtung zur Umsetzung technisch-organisatorischer Maßnahmen zum Schutz vor Störungen der Verfügbarkeit, Integrität und Vertraulichkeit informationstechnischer Systeme und zur Risikominimierung im Falle von Sicherheitsvorfällen vor. Hierunter fallen neben der Einrichtung eines Informationssicherheitsmanagementsystems auch die Durchführung von Risikoanalysen sowie die Erstellung eines Konzepts zur Bewältigung von Sicherheitsvorfällen, ein Konzept zur Gewährleistung der Sicherheit der Lieferkette, die Schulung von Mitarbeitern, Zugriffskontrollen für Personal und Dritte sowie den Einsatz Kryptografie und Verschlüsselungsmethoden und Multi-Faktor-Authentifizierungen.

Die konkret zu ergreifenden Risikomanagementmaßnahmen werden künftig über Durchführungsrechtsakte der EU-Kommission und vom BMI durch Rechtsverordnung (sektorspezifisch) präzisiert und erweitert. In diesem Zusammenhang werden insbesondere etablierte Branchenstandards wie etwa ein nach ISO-270001 zertifiziertes Informationsmanagementsystem eine erhebliche Praxisrelevanz haben.

**Aus Sicht von Teilnehmern an der vertragsärztlichen Versorgung** …
… stehen diese Vorgaben neben der durch die von der Kassenärztlichen Bundesvereinigung erlassenen „Richtlinie nach § 75b SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit“ (IT-Sicherheitsrichtlinie) zur Gewährleistung der IT-Sicherheit. Die IT-Sicherheitsrichtlinie formuliert – abhängig von deren Größe – konkrete technische Vorgaben zur Datenverarbeitung durch vertragsärztliche Praxen (z. B. Einrichtung einer Firewall sowie Vorgaben zu Softwareupdates, der Nutzung von Office-Produkten, der Browsereinstellungen). Die Vorgaben aus dem NIS-2-UmsCG sind im Vergleich zu den – insbesondere gerätebezogenen – Anforderungen aus der IT-Sicherheitsrichtlinie zwar unspezifischer, aber gleichzeitig gerade mit Blick auf die zu ergreifenden organisatorischen Maßnahmen (insbes. Information Security Management System, Sicherheit der Lieferkette) deutlich weitreichender.

Das NIS-2-UmsCG nimmt darüber hinaus auch die **Geschäftsleitung** von Unternehmen in die Pflicht. So soll diese künftig nach § 38 Abs. 1 BSIG-E für die Umsetzung und Überwachung der Risikomanagement verantwortlich sein. Schließlich sieht der Gesetzesentwurf eine Pflicht zur regelmäßigen Teilnahme an Schulungen zu Risiken und Risikomanagementpraktiken im Bereich der Sicherheit der Informationstechnik vor (siehe § 38 Abs. 2 BSIG-E).

## ÜBERWACHUNG UND SANKTIONEN

Das NIS-2-UmsCG gibt dem BSI im Zusammenhang mit der Einhaltung der Pflichten, jedenfalls bei Verdacht auf Nichterfüllung, verschiedene Aufsichts- und Durchsetzungsmaßnahmen an die Hand (vgl. § 62, 61 BISG-E). Hierunter fallen etwa Audits und Prüfungen durch das BSI oder unabhängige Stellen. Das BSI kann künftig zudem auch Nachweise über die Erfüllung etwa der Risikomanagementmaßnahmen verlangen; dies allerdings frühstens 3 Jahre nach dem Inkrafttreten des Gesetzes.

Das BSIG-E sieht diverse Ordnungswidrigkeitstatbestände für die Nicht-Erfüllung der festgesetzten Pflichten vor. Das nicht ordnungsgemäße Umsetzen von Risikomanagementmaßnahmen kann etwa für wichtige Einrichtungen mit einer Geldbuße von bis zu 7 Mio. Euro oder 1,4 % des weltweiten Jahresumsatzes geahndet werden.

Ein finanzielles Risiko besteht auch für die Geschäftsleitung: Diese soll nach § 38 Abs. 2 BSIG-E dem Unternehmen unmittelbar für Schäden haften, die aus der eigenen Pflichtverletzung, etwa der nicht ordnungsgemäßen Umsetzung von Risikomanagementmaßnahmen, entstehen (vgl. § 38 Abs. 2 BSIG-E). Eine D&O Versicherung oder vergleichbare Absicherung ist auch in diesem Zusammenhang unerlässlich. Wichtig zu beachten ist, dass diese jedoch nicht bei grober Fahrlässigkeit und Vorsatz der Geschäftsführung greift. Dies etwa, wenn sich im Einzelfall objektiv aufdrängende Risikomanagementmaßnahmen schlicht nicht umgesetzt werden.

## AKTUELLER HANDLUNGSBEDARF

Pflichten nach dem NIS-2-UmsuCG entstehen erst ab dessen Inkrafttreten. Derzeit nicht ausgeschlossen ist, dass dieser Zeitpunkt noch innerhalb dieser Legislaturperiode eintritt. Ab dessen Inkrafttreten greifen die Pflichten nach dem NIS-2-UmsuCG jedenfalls unmittelbar. Ab dann läuft auch die Registrierungspflicht für (besonders) wichtige Einrichtung, sofern sie die entsprechenden Einordnungskriterien erfüllen (vgl. § 33 Abs. 1 Satz 1 BSIG-E).

Ein dringender Handlungsbedarf der Geschäftsleitung von (potenziell) betroffenen Einrichtungen besteht damit zurzeit *noch* nicht. Dennoch ist größeren ambulanten Einheiten in der ärztlichen Versorgung zumindest eine erste Auseinandersetzung mit dem Thema „Cybersicherheit im Unternehmen“ anzuraten. Mit der Lektüre dieses Artikels haben Sie hierzu bereits einen wesentlichen Beitrag geleistet.

Wir empfehlen im Übrigen die folgenden Handlungsschritte:

**Schritt 1: Klärung der künftigen Betroffenheit nach dem NIS-2-UmsuCG**
*Zumindest größere und/oder umsatzstarke MVZ und Berufsausübungsgemeinschaften sollten klären, ob sie künftig als Betroffene unter das neugefasste BISG fallen könnten.*

**Schritt 2: Weiterbildung zum Thema „Cybersicherheit im Unternehmen“**
*Bilden Sie sich, falls nicht schon geschehen, zu den technischen und organisatorischen Anforderung an die Cybersicherheit in Unternehmen fort oder übertragen Sie diese Aufgabe an einen zuverlässigen Mitarbeiter.*

**Schritt 3: Bestandsaufnahme zur Cybersicherheit im eigenen Unternehmen**
*Klären Sie – idealerweise unter Einschaltung fachmännischer Unterstützung – den aktuellen Stand der Cybersicherheit in Ihrem Unternehmen.*

**Schritt 4: Ggf. Schließung zumindest eklatanter Sicherheitslücken**
*Offenbaren sich im vorstehenden Schritt eklatante Lücken, empfiehlt sich schon im Eigeninteresse die Einleitung entsprechender Gegenmaßnahmen.*

**Schritt 5: Regelmäßige Information dem Gang des Gesetzgebungsverfahrens**
*Halten Sie über die weitere Entwicklung des Gesetzgebungsverfahrens informiert.*

**Kontakt zu den Autoren**

**Rechtsanwälte** Dr. Thomas **Willaschek |** Sebo-Franz **Krubally**
030 – 521 33 24925| thomas.willaschek@luther-lawfirm.com

*Luther Rechtsanwaltsgesellschaft mbH*
Heidestr. 40 | 10557 Berlin | **www.luther-lawfirm.com**