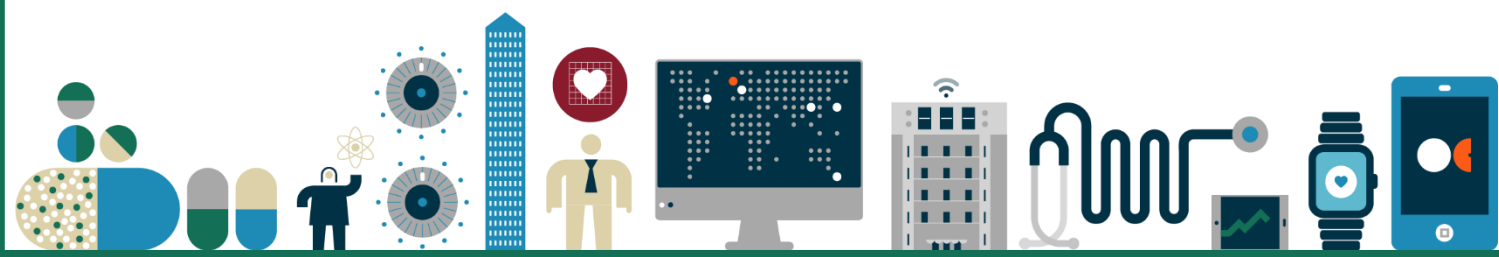
Die Umsetzung der NIS-2-Richtlinie in Deutschland schreitet voran – was bedeutet das für Life-Sciences- & Healthcare-Unternehmen?

1. IT-Sicherheit wird immer wichtiger – der Kreis verpflichteter Unternehmen wird erheblich erweitert

- Die Bundesregierung hat am 24. Juli 2024 einen Gesetzentwurf („**BSIG-neu**“) zur Umsetzung der Richtlinie (EU) 2022/2055 („**NIS-2**“) veröffentlicht. Wesentliche Vorgaben von NIS-2 werden im BSIG-neu, dem neu gefassten Gesetz über das Bundesamt für Sicherheit in der Informationstechnik, umgesetzt.
- Betroffene Unternehmen sind zur Umsetzung geeigneter, verhältnismäßiger und wirksamer technischer und organisatorischer Maßnahmen zum Schutz ihrer IT-Systeme verpflichtet. Darüber hinaus sind sie zur Registrierung beim BSI, zur Meldung von erheblichen Sicherheitsvorfällen innerhalb von 24 Stunden an das BSI sowie zur Information der Kunden bei erheblichen Sicherheitsvorfällen verpflichtet, soweit vom BSI angeordnet. Die Geschäftsleitung ist dafür verantwortlich, die ordnungsgemäße Umsetzung der IT-Sicherheitspflichten sicherzustellen und zu überwachen.
- Den Pflichten des BSIG-neu können Unternehmen grundsätzlich unterfallen, wenn sie mehr als 50 Mitarbeiter beschäftigen oder einen Jahresumsatz und eine Jahresbilanzsummer von jeweils über EUR 10 Mio. aufweisen.

2. Welche Life-Sciences- & Healthcare-Unternehmen dem BSIG-neu unterfallen können

- Sofern die erforderlichen Schwellenwerte erreicht werden, können nach Anlage 1 und 2 zum BSIG-neu folgende Life-Sciences- & Healthcare-Unternehmen als besonders wichtige Einrichtungen oder wichtige Einrichtungen den Pflichten des BSIG-neu unterfallen:
    - Erbringer von Gesundheitsdienstleistungen wie z.B. Krankenhäuser oder Fachkliniken
    - EU-Referenzlaboratorien nach Art. 15 der Verordnung (EU) 2022/2371
    - Unternehmen aus dem Bereich der Arzneimittelforschung und -entwicklung
    - Hersteller von pharmazeutischen Erzeugnissen, pharmazeutischen Grundstoffen oder pharmazeutischen Spezialitäten und sonstigen pharmazeutischen Erzeugnissen
    - Hersteller von kritischen Medizinprodukten nach Art. 22 der Verordnung (EU) 2022/123
    - Hersteller von Medizinprodukten und In-vitro-Diagnostika
    - Forschungseinrichtungen
- Nach dem BSIG-neu fallen unter die Kategorie der besonders wichtigen Einrichtungen auch "kritische Anlagen“, die noch durch eine neue Verordnung zu bestimmen sind. Es ist aber wahrscheinlich, dass diejenigen Anlagen, die unter der bisherigen BSI-KritisV als „kritische Infrastrukturen“ qualifiziert wurden, auch zukünftig als "kritische Anlagen" unter dem BSIG-neu zu qualifizieren sind. Diese Erweiterung des Anwendungsbereichs geht zurück auf Art. 2 Abs. 3 NIS-2.

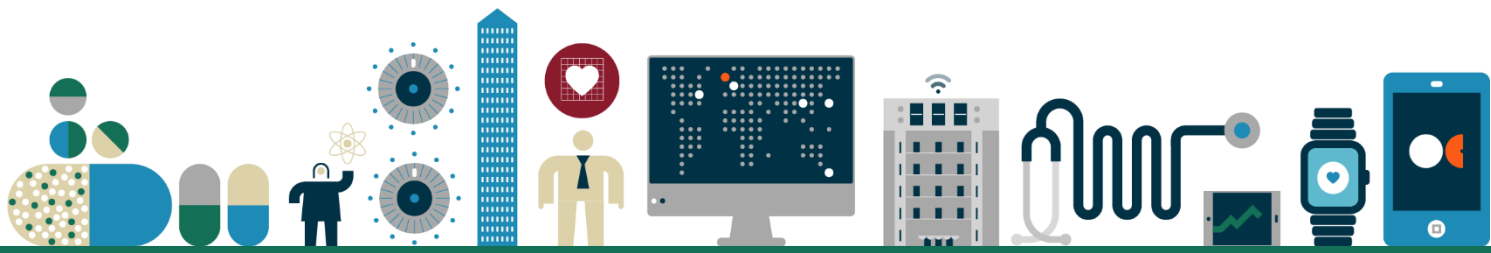


3. Das BSIG-neu im Kontext sektorspezifischer Vorgaben: Cyber Resilience Act, Medizinprodukteverordnung (MDR) EU-VO 2017/745 etc.

- Das BSIG-neu lässt die Anwendung der MDR unberührt und findet neben ihr Anwendung auf Medizintechnikunternehmen, soweit diese die erforderlichen Schwellenwerte erreichen bzw. überschreiten.
- Wegen seiner unterschiedlichen Schutzrichtung und seines produktspezifischen Ansatzes werden die Vorgaben des Cyber Resilience Acts (*laufendes Gesetzgebungsverfahren*) neben den IT-sicherheitsrechtlichen Vorgaben des BSIG-neu anwendbar sein. Medizintechnikprodukte mit digitalen Elementen, die bereits unter die MDR fallen, sowie In-vitro-Diagnostika werden allerdings vom Anwendungsbereich des CRA ausgenommen sein.
- Die besonderen IT-Sicherheitspflichten für Krankenhäuser nach § 391 SGB V sowie für Anbieter Digitaler Gesundheitsanwendungen (DIGA) nach der DiGAV bleiben grds. bestehen, werden aber an die Vorgaben des BSIG-neu angepasst und erweitert.

4. Handlungsempfehlungen für potenziell betroffene Akteure

- Life-Sciences- & Healthcare-Unternehmen sollten zunächst prüfen, ob sie dem Anwendungsbereich des BSIG-neu unterfallen (ggf. auch durch Tätigkeiten außerhalb des Kerngeschäfts, wie z.B. Verwaltung konzerneigener IT-Infrastruktur). Das BSI bietet mit einem speziellen Tool eine erste Orientierung und stellt auch weiterführende Informationen im Zusammenhang mit der Umsetzung von NIS-2 zur Verfügung.
- Zur Umsetzung der Vorgaben des BSIG-neu sollte ein Projektteam etabliert werden, das die Umsetzung von Informationssicherheitsmaßnahmen im Unternehmen koordiniert.
    - Mitarbeitende der IT-, Kommunikations- und Rechtsabteilung sollten frühzeitig involviert werden.
    - Anders als bisher kommt auch der Unternehmensleitung wesentliche Bedeutung zu (IT-Sicherheit wird „Chefsache“).
- Die Durchführung einer Bestandsaufnahme in Sachen Informationssicherheit im Unternehmen (inkl. der Lieferkette) kann helfen, einen Handlungsplan mit Zeitvorgaben zur konkreten Umsetzung der Vorgaben des BSIG-neu zu entwickeln und das hierfür erforderliche Budget zu identifizieren (ggf. kann hierfür auf Erfahrungen aus der Vorbereitung auf die DS-GVO zurückgegriffen werden).
- Besonderes Augenmerk sollten betroffene Unternehmen auf die frühzeitige Durchführung von Risikobewertungen, die Implementierung von Prozessen zur Reaktion auf IT-Sicherheitsvorfälle und die Sensibilisierung der Mitarbeiter (und der Geschäftsführung) für die Belange der IT-Sicherheit richten.



Ihre Experten

Julia Kaufmann, LL.M. (Univ. of Texas)
Partner, München

T +49 89 5434 8068
julia.kaufmann@osborneclarke.com

Dr. Tobias Rothkegel
Partner, Hamburg

T +49 40 55436 4090
tobias.rothkegel@osborneclarke.com

Dr. Florian Eisenmenger
Counsel, München

T +49 89 5434 8108
florian.eisenmenger@osborneclarke.com