HEUKING

NIS-2 Richtlinie

Erste Pflichten greifen
ab Oktober 2024

Was müssen Unternehmen beachten?

Dr. Hans Markus Wulf
Rechtanwalt | Partner
Fachanwalt für IT-Recht
Datenschutzauditor (TÜV)

HEUKING

Was regelt die NIS-2-Richtlinie?

Inhalt

Die NIS-2-Richtlinie stellt neue Regeln auf zur Cyber- und Informationssicherheit für Unternehmen, die im Zusammenhang mit kritischen Infrastrukturen tätig sind.

Welche Bereiche sind als kritische Infrastruktur umfasst?

Die revelanten Bereiche ergeben sich aus Anlage 1 und 2 des anstehenden Umsetzungsgesetzes. Derzeit sind dies insb. Energie, Transport/Verkehr, Finanz-/Versicherungswesen, Gesundheit, Wasser/Abwasser, IT/TK, Weltraum (Anlage 1) sowie Siedlungsabfallentsorgung, chemische Stoffe, Lebensmittel, Medizinprodukte/In-Vitro-Diagnostika, DV, Maschinenbau, Automotive, digitale Dienste und Forschung (Anlage 2)

Fristen

Die NIS-2-Richtlinie wurde bereits am 27.12.2022 veröffentlicht. Sie muss bis Oktober 2024 umgesetzt sein. Der Entwurf des deutschen Umsetzungsgesetzes (NIS2-UmsuCG-E) sieht bislang keine Übergangsfristen vor. Insoweit sind die Vorgaben intern bis Oktober, extern (Registrierung) bis Januar 2025 umzusetzen.

Aufsicht

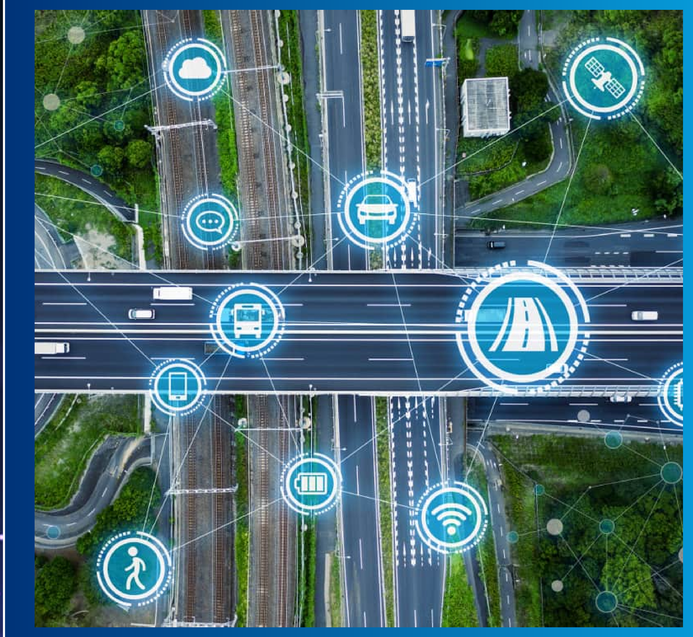
Zuständige Behörde in Deutschland wird das BSI sein (Bundesamt für Sicherheit in der Informationstechnik).

Bußgelder

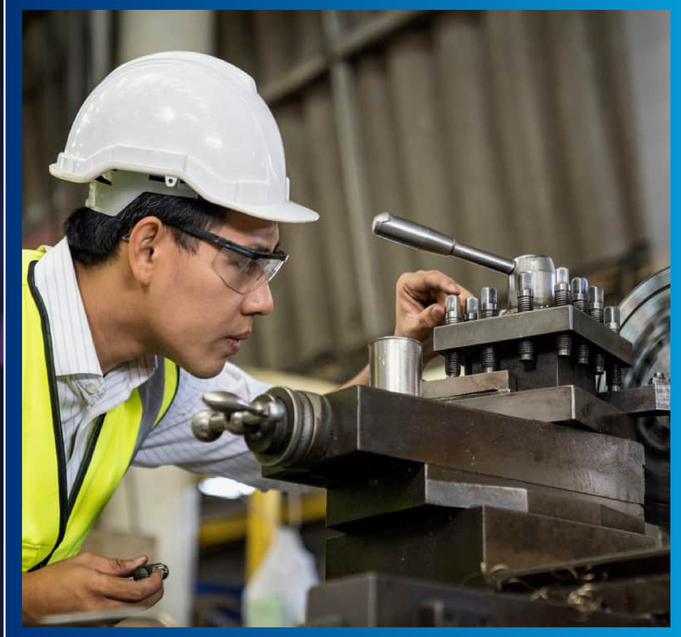
Verstöße gegen die neuen NIS-2-Vorgaben können mit Bußgeldern bis zu EUR 10 Mio. bzw. 2% des weltweiten Jahresumsatzes geahndet werden (besonders wichtige Einrichtungen) sowie EUR 7 Mio. bzw. 1,4% (wichtige Einrichtungen, ca. 21.000 Unternehmen in Deutschland).

HEUKING

Wer muss u.a. handeln?



KRITIS-BETREIBER z.B.
Energie, Verkehr, Banken



MASCHINENBAU-
UNTERNEHMEN*

Anbieter von
GESUNDHEITSDIENSTEN*

Anbieter von CLOUD-
DIENSTEN*

Anbieter von MANAGED
SERVICES*

Anbieter von DIGITALEN
DIENSTEN (zB Marktplätze)*

* wenn mehr als 50 Mitarbeiter
oder mehr als EUR 10 Mio.
Jahresumsatz und -bilanzsumme

HEUKING

Was sind wichtige Pflichten?

Registrierung beim BSI, § 33

Einführung von speziellem Risikomanagement-System (insb. ISMS wie ISO 27001, § 30 II Nr. 1c*)

Einrichtung von Meldesystem für Sicherheitsvorfälle, teilweise Fristen von 24 Stunden nach Kenntnis, § 32

Einrichtung von Governancesystem durch Geschäftsführer/Vorstand, persönliche Haftung, § 38

umfassende Informationspflichten ggü. Kunden, § 35

Umsetzung technischer und organisatorischer Sicherheitsmaßnahmen, z.B. Konzept zum Einsatz von Verschlüsselung, Verfahren zur Cyberhygiene oder Schulung von Mitarbeitern, § 30

* NIS2UmsuCG-E

HEUKING

Was sind wichtige Schritte hin zu einer NIS-2-Compliance ?

Leitlinie

- Erstellung von IT-Sicherheitsrichtlinie
- Erstellung von Überprüfungsprozess zur Einhaltung der Richtlinie

Governance

- Festlegung von Verantwortlichkeiten
- Aufgabentrennung
- Security by Design
- Risikobewertungen

Personal

- Sicherheitsprüfung von Bewerbern
- IT-Sicherheit in Arbeitsverträgen
- Schulungen
- Maßregelungsprozess

Betriebsmittel

- Inventarisierung IT-relevanter Betriebsmittel
- Zuständigkeiten
- Richtlinie zu Gebrauch und Rückgabe

Daten

- Klassifizierung und Kennzeichnung von Daten
- Richtlinie zum Umgang mit Daten

Zugang

- Zugangssteuerungs-richtlinie
- Nutzerverwaltung
- Verantwortlichkeiten
- Zugang zu Systemen

Kryptographie

- Richtlinie zum Gebrauch krypto-grafischer Maßnahmen
- Schlüsselverwaltung

Physische Sicherheit

- Festlegung von Sicherheitsbereichen
- Physische Sicherheit
- Gerätesicherheit
- Arbeitsumgebung

Betriebssicherheit

- Sichere Betriebsabläufe
- Schutz v. Schadsoftware
- Datensicherung
- Protokollierung
- Updateprozesse
- Audits

Kommunikation

- Netzwerksicherheit
- Richtlinie zur Datenübertragung
- Auftragsverabeitung
- Geheimhaltung

Systeme

- Anforderungen an Beschaffung festlegen
- Richtlinie für sichere Entwicklung
- Testverfahren
- Schutz von Testdaten

Lieferanten

- IT-Sicherheitsrichtlinie für Lieferantenbeziehungen (Lieferkette)
- Überwachung von Dienstleistern
- Änderungsverfahren

Vorfälle

- Richtlinie zum Umgang mit Sicherheitsvorfällen
- Festlegung von Verantwortlichkeiten
- Meldeverfahren
- Incident-Management

Business Continuity

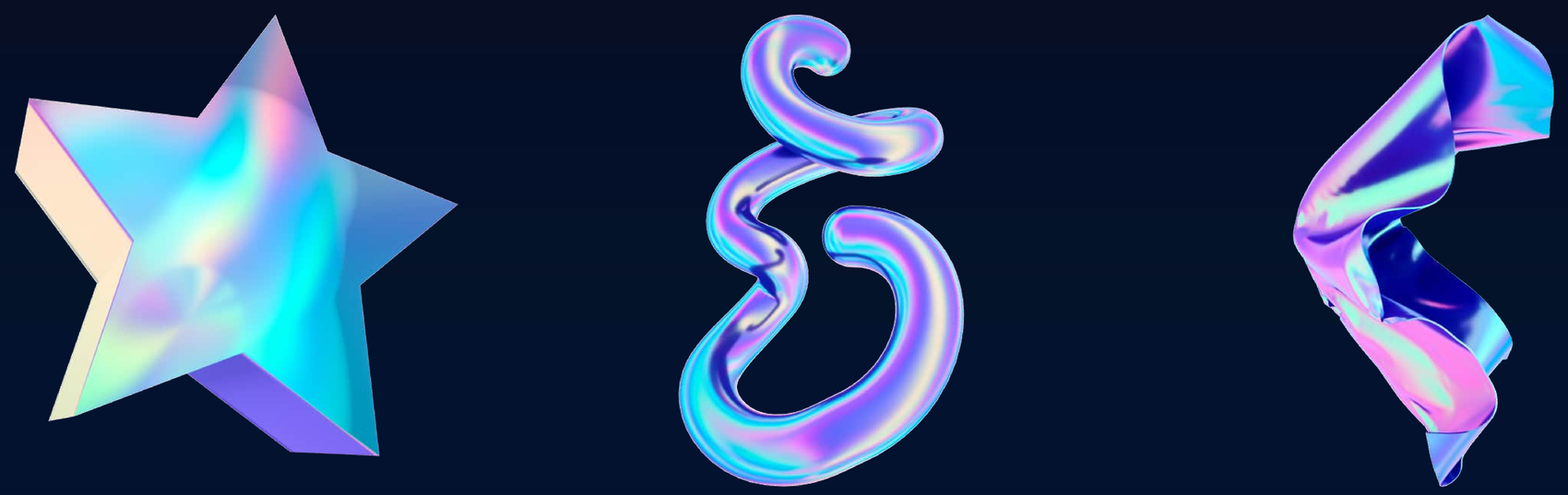
- Festlegung von Anforderungen
- Erstellung von BC-Richtlinie
- Festlegung von Überprüfungsprozess

Compliance

- Ermittlung geltender Gesetzesvorgaben
- Sicherung v. IP-Rechten
- Dokumentation
- Audits

HEUKING

Wie können Experten von HEUKING unterstützen?



Beratung, Schulungen

Webinare, Inhouse-Seminare, Workshops zur Umsetzung der NIS-2-Vorgaben, Steuerung des Implementierungs-prozesses, etwa zur Einführung eines Information-Security-Management-Systems (ISMS)

NIS-2-Compliance-Paket

Richtlinien, Checklisten, Vertragsmuster, Vorlagen für Risikobewertungen

Durchführung von Audits zur Einhaltung der NIS-2-Compliance

Behörden-Kommunikation

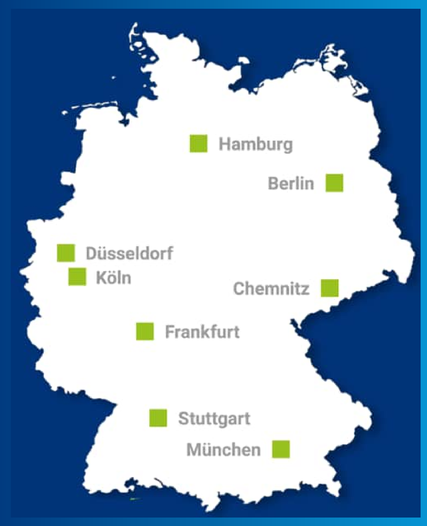
Fallstricke vermeiden: Wir übernehmen die Korrespondenz

HEUKING hat viele ISMS-Projekte begleitet, mehrere Anwälte verfügen über zertifizierte ISO-27001-Expertise.

Die Sozietät

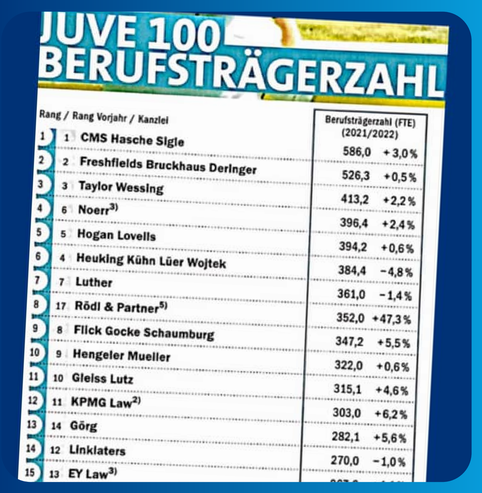
HEUKING

400+
Rechtsanwälte
Steuerberater
Notare



8
Standorte

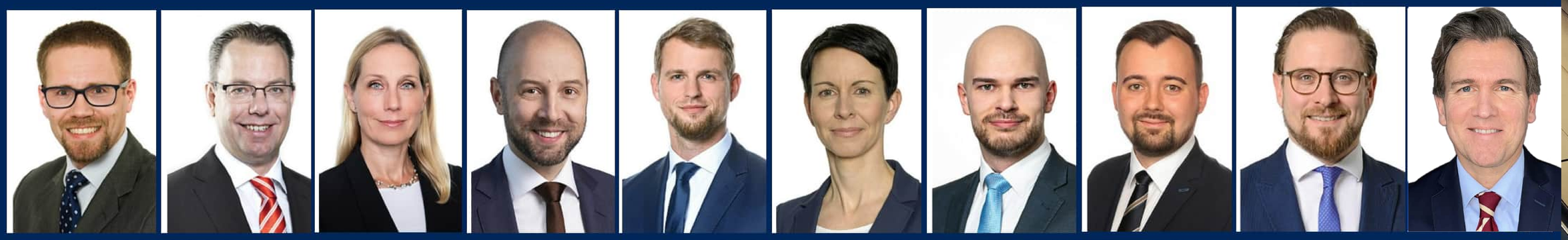
98
Partnerkanzleien
weltweit



Ausgezeichnet

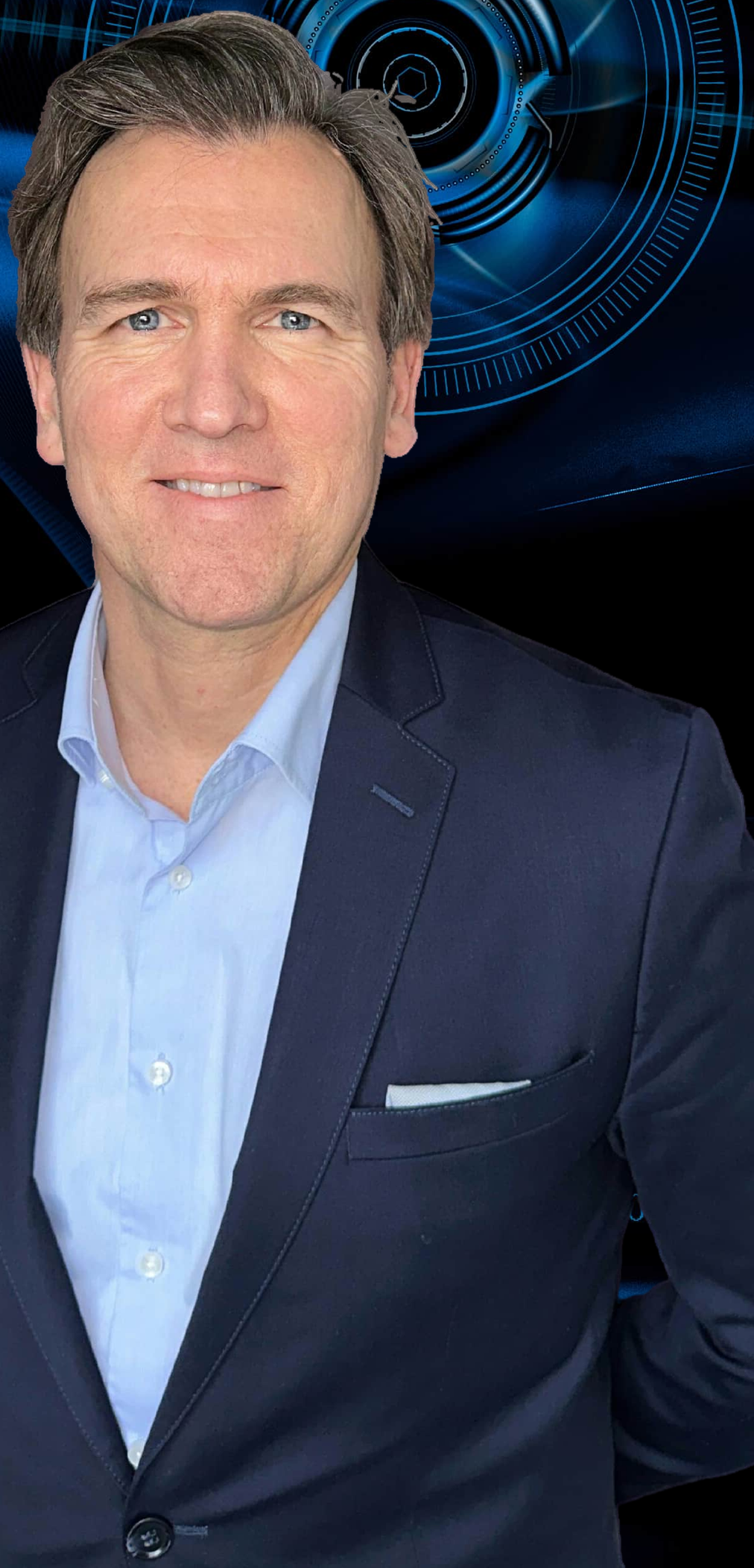
JUVE TOP 50 Wirtschaftskanzlei Deutschland 2023|2024 · The LEGAL 500 DEUTSCHLAND TOP KANZLEI 2023 · BEST OF LEGAL 2023 DEALS 1. PLATZ Wirtschafts Woche · Chambers TOP RANKED Europe 2023 Heuking Kühn Lüer Wojtek

20 von 400: HEUKING Technologie-Rechtsexperten



HEUKING

Sprechen Sie uns gern an.



Kontakt

Dr. Hans Markus Wulf
Rechtsanwalt, Partner
Fachanwalt für IT-Recht
Datenschutzauditor (TÜV)

+49 40 355280-980

www.heuking.de

m.wulf@heuking.de

Heuking Kühn Lüer Wojtek PartG mbB
Neuer Wall 63, 20354 Hamburg