TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

TeleTrusT-"IT-Sicherheitsrechtstag" 2024

Berlin, 25.09.2024

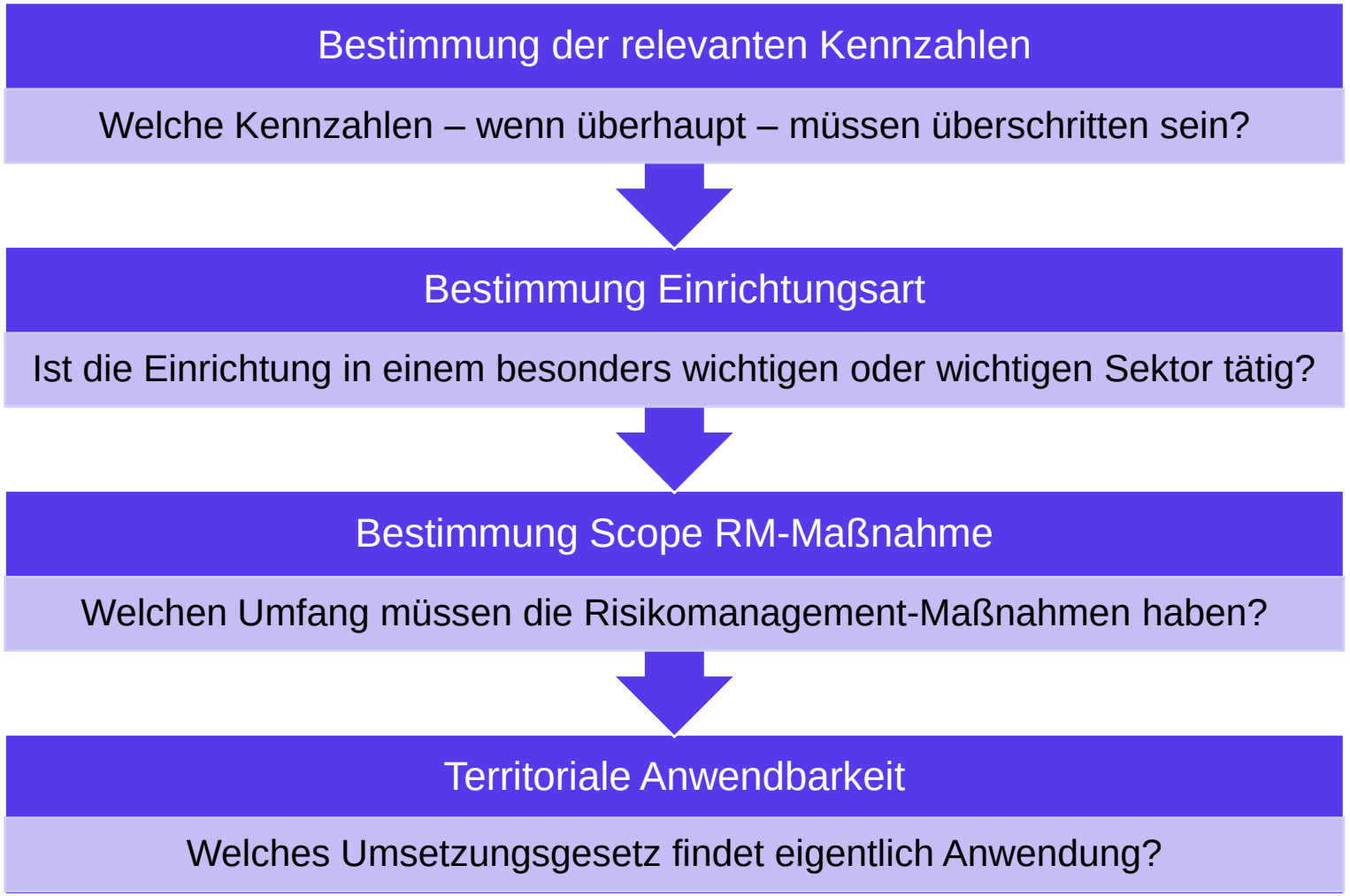
NIS2-Umsetzungsgesetz: Eine Frage der Anwendbarkeit

RA Julian Monschke, Noerr Partnerschaftsgesellschaft mbB

Content

Fragen der Anwendbarkeit im Überblick

Ein Überblick über die Fragen der Anwendbarkeit



Überblick über die relevanten Sektoren

Sektoren mit hoher Kritikalität (Anhang I der NIS2-RL)	Sonstige kritische Sektoren (Anhang II der NIS2-RL)
Energie	Post- und Kurierdienste
Verkehr	Abfallbewirtschaftung
Bankwesen	Produktion, Herstellung und Handel mit chemischen Stoffen
Finanzmarktinfrastrukturen	Produktion, Verarbeitung und Vertrieb von Lebensmitteln
Gesundheitswesen	Verarbeitendes Gewerbe/Herstellung von Waren
Trinkwasser	Anbieter digitaler Dienste
Abwasser	Forschung
Digitale Infrastruktur	
Verwaltung von IKT-Diensten (B2B)	
Öffentliche Verwaltung	
Weltraum	

Grundfall der Bestimmung relevanter Kennzahlen

Besonders wichtige Einrichtungen

Der Grundfall für besonders wichtige Einrichtungen:

- **Anlage 1**-Tätigkeit und
- mindestens 250 **Mitarbeiter:innen** (FTE, vgl. Art. 5 KMU-Empfehlung) **oder**
- **Jahresumsatz** von über EUR 50 Mio. und eine **Jahresbilanzsumme** von über EUR 45 Mio.
- *Sonderfälle gelten für kritische Anlagen, TK-Dienste/Netze und weitere Spezialfälle*

Wichtige Einrichtungen

Der Grundfall für wichtige Einrichtungen

- **Anlage 1 oder 2**-Tätigkeit und
- Mindestens 50 **Mitarbeiter:innen oder**
- **Jahresumsatz** und eine **Jahresbilanzsumme** von jeweils mindestens EUR 10 Mio.
- *Sonderfälle gelten für kritische Anlagen, TK-Dienste/Netze und weitere Spezialfälle*

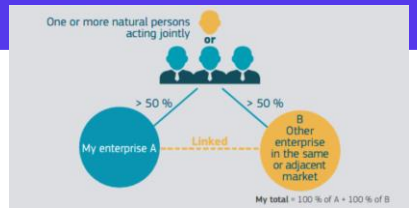
Mythos 1: „*Mein Unternehmen hat über 250 Mitarbeitende, daher sind wir eine besonders wichtige Einrichtung.*“

Mythos 2: „*Jedes Unternehmen, das eine Anlage 1-Tätigkeit ausführt, ist eine besonders wichtige Einrichtung.*“

Besonderheiten der Bestimmung

Grundsatz

- Zurechnung im Konzern
- Grundsatz: Zurechnung der Kennzahlen im Konzern
- In der Regel „*Verbundene Unternehmen*“ im Sinne der KMU-Empfehlung (siehe dazu ergänzend: https://op.europa.eu/s/zScW)



Ausnahme

- Keine Zurechnung im Konzern
- Bei einer unabhängigen IT findet **keine** Zurechnung von Partner- und Verbundenen Unternehmen statt (§ 28 Abs. 3 Nr. 2 BSIG-E)

Einrichtungsart

- Eine deutsche Besonderheit
- Es ist auf „*die der Einrichtungsart zuzuordnende Geschäftstätigkeit abzustellen*“ (§ 28 Abs. 3 Nr. 1 BSIG-E)
- Europarechtskonformität sehr fraglich
- Zurechnung im Konzern unklar

Besonderheiten bei der Bestimmung der Einrichtungsarten
Chemie-Sektor

Abweichung im Chemie-Sektor:

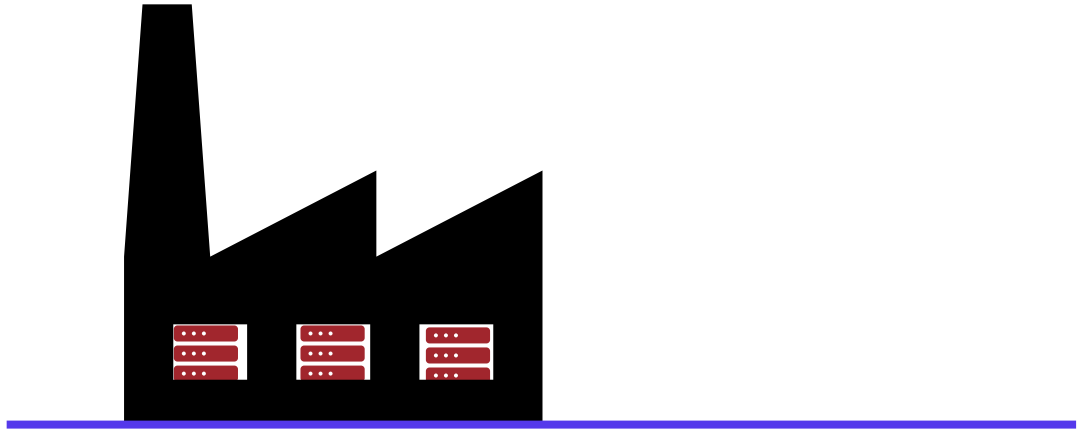
- NIS2-RL: „*Unternehmen im Sinne des Artikels 3 Nummern 9* [Hersteller] *und 14* [Händler] *der REACH-VO, die Stoffe herstellen und mit Stoffen oder Gemischen handeln, und Unternehmen, die Erzeugnisse im Sinne des Artikels 3 Nummer 3 der genannten Verordnung aus Stoffen oder Gemischen produzieren*“
- BSIG-E: „*Hersteller und Importeure nach Artikel 3 Nummern 9 und 11 der [REACH-VO] von chemischen Stoffen und Gemischen im Sinne des Artikels 3 Nummer 1 und 2 der genannten Verordnung,* ***sofern*** *diese in Kategorie 20 der […] NACE Rev. 2 fallen*“

Besonderheiten bei der Bestimmung der Einrichtungsarten
Rechenzentren

Abweichende Definition Rechenzentrum:

- NIS2-RL: „*einen Dienst, mit dem spezielle Strukturen oder Gruppen von Strukturen für die zentrale Unterbringung, die Verbindung und den Betrieb von IT- und Netzausrüstungen zur Erbringung von Datenspeicher-, Datenverarbeitungs- und Datentransportdiensten sowie alle Anlagen und Infrastrukturen für die Leistungsverteilung und die Umgebungskontrolle bereitgestellt werden* “
- BSIG-E: „*ein Dienst, der Strukturen umfasst, die dem vorrangigen Zweck der zentralen Unterbringung, der Zusammenschaltung und dem Betrieb von IT- oder Netzwerkausrüstungen dienen, und die* ***Datenverarbeitungsdienste*** *erbringen, mitsamt* ***allen benötigten*** *Anlagen und Infrastrukturen, insbesondere für die* ***Stromverteilung*** *und die Umgebungskontrolle*“ (Regierungsbegründung: „*Die Datenverarbeitung umfasst dabei insbesondere auch Transport und Speicherung*“)

Scope der Risiko-Management Maßnahmen



Im wesentlichen zwei Auslegungsergebnisse:

- Gesamtes Unternehmen muss NIS2-Maßnahmen ergreifen
- Nur die Systeme, *Komponenten und Prozesse* müssen gesichert werden, die für die relevante(n) Einrichtungsart(en) genutzt werden

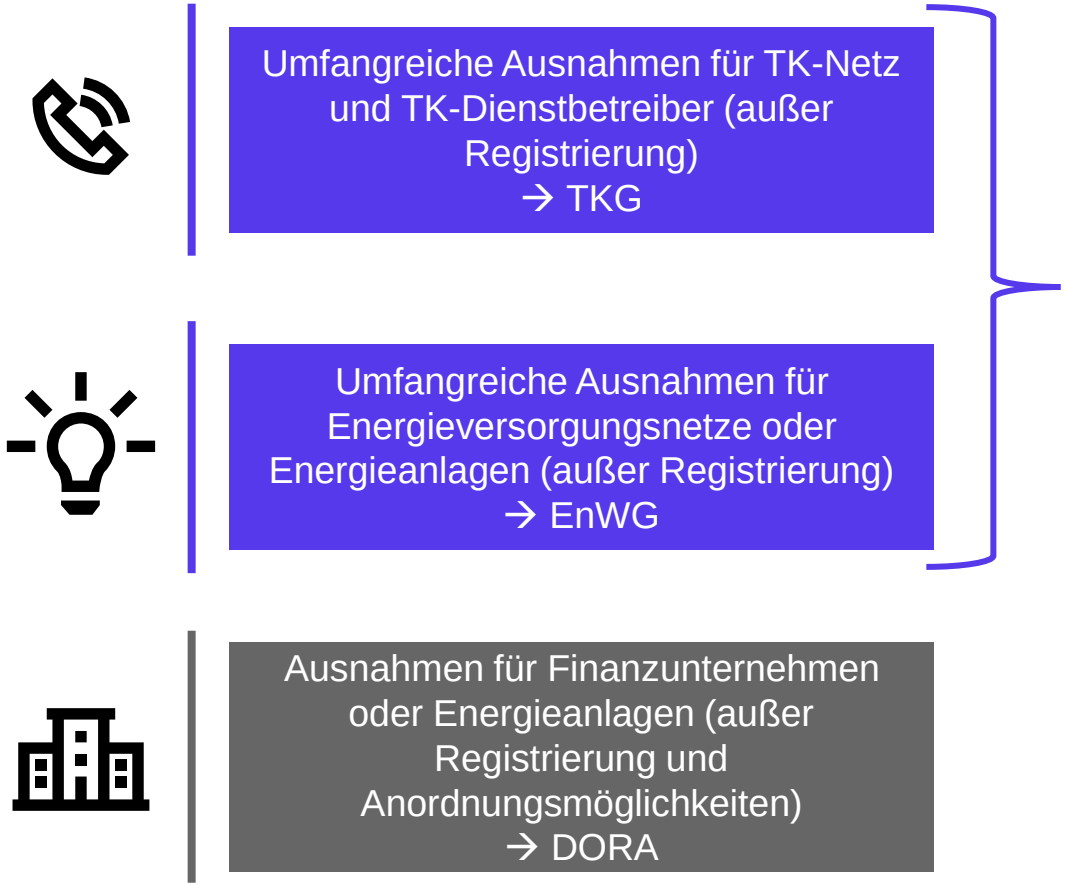
Deutsche Gesetzesbegründung:

„*in Folge der Umsetzung der NIS-2-Richtlinie [sind] zukünftig sämtliche informationstechnischen Systeme, Komponenten und Prozesse zu berücksichtigen, die von der jeweiligen Einrichtung für die Erbringung ihrer Dienste genutzt werden. Der Begriff „Erbringung ihrer Dienste“ ist hierbei weit gefasst*“ […]“

Territoriale Anwendbarkeit des NIS2-Umsetzungsgesetzes

- **Grundsatz**: Ort der Niederlassung (Art. 26 Abs. 1 NIS2-RL)
- Anbieter von **TK-Netzen/TK-Diensten**: Zuständigkeit **aller** Behörden, in denen die Dienste erbracht werden
- Diverse „**Digital-Dienste**“: Ort der Hauptniederlassung („Steuerung“ der IT)
- Einrichtungen ohne Niederlassung in der Union müssen einen Vertreter in der Union benennen

Abweichende Regelungen für bestimmte Sektoren



…und wie werden Kritische Anlagen definiert?

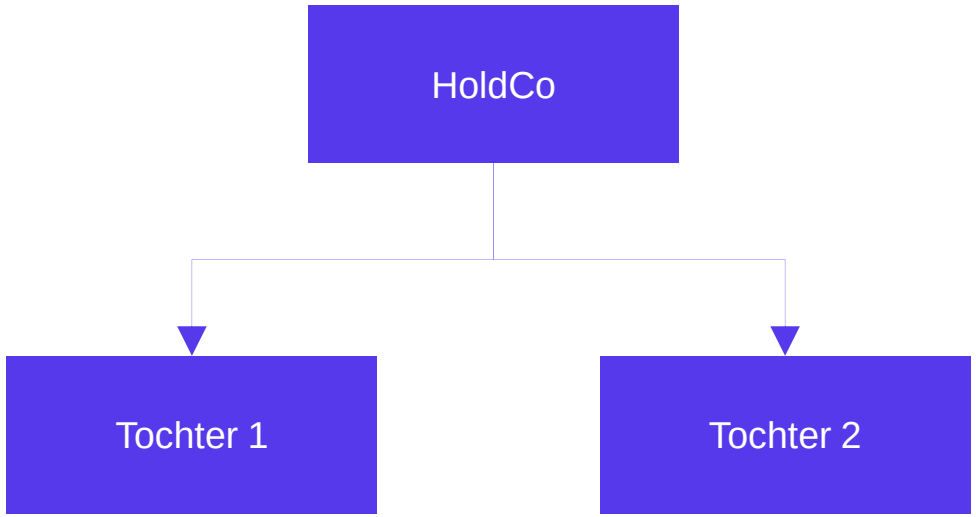
- Grundsätzlich bleibt es dabei, dass eine Rechtsverordnung zur Bestimmung notwendig bleibt
- Voraussichtlich wird die heute geltende KRITIS-Verordnung fortgelten (unklar, nicht eindeutig so aus Regierungsentwurf ersichtlich)
- Gleichlauf der KRITIS-Verordnung für BSIG-E und KRITIS-DachG-E (nach § 4 Abs. 4 KRITIS-DachG-E bis 17. April 2026)

Anwendbarkeit des NIS2-Umsetzungsgesetzes in Fällen

Ein moderner Klassiker: Die konzerninterne IT-Infrastruktur

Sachverhalt	Lösungsansätze
– Eine Konzernobergesellschaft betreibt (nur) für andere Konzerngesellschaften ein Rechenzentrum – **Variante**: Die Konzernmutter ist nur Vertragsinhaber für diverse IT-Leistungen, die die Tochtergesellschaften beziehen können	– Erwägungsgrund 35 NIS2-RL: gilt „*nicht für interne Rechenzentren, die sich im Besitz der betreffenden Einrichtung befinden und von der betreffenden Einrichtung für eigene Zwecke betrieben werden*“ – **Variante**: Wohl kein eigenes Angebot eines RZ (aber MSP?)
– Die zentrale IT-Abteilung kümmert sich um alle Belange der Gruppe. Die Abteilung installiert bspw. Software auf den Endgeräten der Gruppe. – Ein Unternehmen mietet sich ein neues Bürogebäude und wird Flächen untervermieten. Es plant, Kommunikationssysteme mitzuvermieten (etwa WLAN-AP).	– Vieles spricht dafür, dass beide Unternehmen dann zum Managed Service Provider werden; ggf. auch Managed Security Provider – „*Dienste im Zusammenhang mit der Installation, der Verwaltung, dem Betrieb oder der Wartung von IKT-Produkten, -Netzen, -Infrastruktur, -Anwendungen oder jeglicher anderer Netz- und Informationssysteme durch Unterstützung oder aktive Verwaltung in den Räumlichkeiten der Kunden oder aus der Ferne*“ (§ 2 Nr. 26 BSIG-E)

Szenarien in einer Unternehmensgruppe



- **Szenario 1**: Die HoldCo betreibt für die gesamte Gruppe IT-Leistungen, etwa ein Rechenzentrum → **Siehe soeben**
- **Szenario 2**: Eine der links genannten Gesellschaften betreiben Geschäft in einer relevanten Einrichtungsart, aber überschreiten jeweils nicht alleine die relevanten Schwellenwerte → **Siehe bereits zu Beginn**
- **Szenario 3**: Tochtergesellschaft 1 betreibt nicht selbst die IT sondern die HoldCo, betreibt aber Geschäft in einer relevanten Einrichtungsart → Keine „Infektion“ der HoldCo, aber „Sicherheit in der Supply Chain“

Doch keine explosive Mischung: Verkauf von chemischen Gemischen

Sachverhalt	Lösungsansätze
– Ein Unternehmen verkauft Mittel, bei denen die chemische Struktur im Vordergrund steht (etwa: Frostschutzmittel) – Das Unternehmen produziert diese nicht, sondern verkauft nur	– Definition: „*Hersteller und Importeure nach Artikel 3 Nummern 9 und 11 der [REACH-VO] von chemischen Stoffen und Gemischen im Sinne des Artikels 3 Nummer 1 und 2 der genannten Verordnung, sofern diese in Kategorie 20 der […] NACE Rev. 2 fallen*“ – Mittel wohl noch kein Erzeugnis, sondern eher Gemisch – Unternehmen verkauft nur, stellt aber nicht her → Keine Anwendbarkeit des NIS2-Umsetzungsgesetzes – Abweichend nach NIS2-RL!

Smarte Geräte: Smarte Regulierung

Sachverhalt	Lösungsansätze
– Ein Unternehmen stellt smarte Glühbirnen her. Diese sind (natürlich) jeweils mit dem Internet verbunden. – Zusätzlich stellt das Unternehmen eine Online-basierte Lösung bereit, über die Funktionen der Geräte gesteuert werden können.	– Anlage 2 zum BSIG-E: „Herstellung von elektrischen Ausrüstungen“ nach Abteilung 27 NACE rev. 2 – Klasse 27.40: „*Herstellung von Entladungslampen, Glühlampen, Leuchtstofflampen, Ultraviolettlampen, Infrarotlampen und anderen Lampen und Beleuchtungskörpern*“ – Cloud-Computing-Dienste (§ 2 Nr. 4 BSIG-E): „*ein digitaler Dienst, der auf **Abruf die Verwaltung** eines **skalierbaren und elastischen Pools gemeinsam nutzbarer Rechenressourcen** sowie den umfassenden Fernzugang zu diesem Pool ermöglicht, auch wenn die Rechenressourcen auf **mehrere Standorte** verteilt sind*“

Deep Dive: Cloud Computing Services

- Erwägungsgrund 33 NIS2-RL verweist zur Definition auf ISO/IEC 17788:2014; dieser ist veraltet und ersetzt durch ISO/IEC 22123-1
- Nach BSI sind demnach folgende Kriterien relevant:
  - **Allgemeiner Netzwerkzugang** (*broad network access*): Die Services sind mit Standard-Mechanismen über ein Netz verfügbar und nicht an einen bestimmten Client gebunden.
  - **Messbare Dienste** (*measured service*): Die Ressourcennutzung kann gemessen, überwacht und entsprechend bemessen werden.
  - **Mandantenfähigkeit** (*multi-tenancy*): Die Zuteilung von physischen oder virtuellen Ressourcen erfolgt so, dass die Prozesse und Daten verschiedener Mandanten voneinander getrennt und füreinander unzugänglich sind.
  - **Selbstbedienung auf Anforderung** (*on-demand self-service*): Die Provisionierung der Ressourcen (z. B. Rechenleistung oder Speicher) läuft automatisch ohne manuelle Interaktion des Cloud-Anbieters ab.
  - **Zeitgerechte Elastizität und Skalierbarkeit** (*rapid elasticity and scalability*): Die Cloud-Dienste können schnell und elastisch zur Verfügung gestellt werden, in manchen Fällen auch automatisch. Aus Anwendersicht scheinen die Ressourcen daher unbegrenzt zu sein.
  - **Ressourcenreservoirs** (*resource pooling*): Die Ressourcen des Cloud-Anbieters liegen in einem Pool, aus dem Cloud-Anwender bedient werden (Multi-Tenant Modell).

(Quelle: https://www.bsi.bund.de/dok/6622124)

Smarte Geräte: Smarte Regulierung

Sachverhalt	Lösungsansätze
– Ein Unternehmen stellt smarte Glühbirnen her. Diese sind (natürlich) jeweils mit dem Internet verbunden. – Zusätzlich stellt das Unternehmen eine Online-basierte Lösung bereit, über die Funktionen der Geräte gesteuert werden können.	– Anlage 2 zum BSIG-E: „Herstellung von elektrischen Ausrüstungen“ nach Abteilung 27 NACE rev. 2 – Klasse 27.40: „*Herstellung von Entladungslampen, Glühlampen, Leuchtstofflampen, Ultraviolettlampen, Infrarotlampen und anderen Lampen und Beleuchtungskörpern*“ – Cloud-Computing-Dienste (§ 2 Nr. 4 BSIG-E): „*ein digitaler Dienst, der auf **Abruf die Verwaltung** eines **skalierbaren und elastischen Pools gemeinsam nutzbarer Rechenressourcen** sowie den umfassenden Fernzugang zu diesem Pool ermöglicht, auch wenn die Rechenressourcen auf **mehrere Standorte** verteilt sind*“
	Bonus Regulierung 1: Hersteller eines vernetzten Produkts nach **Data Act**
	Bonus Regulierung 2: Geräte (und Online-Anwendung?) sind vss. Produkte mit digitalen Elementen nach dem **Cyber Resilience Act**

Abschluss

Fazit

- In NIS2-Prüfungen auch an etwaige Nebentätigkeiten des Unternehmens denken
- Unsicherheit durch möglicherweise europarechtswidrige Beschränkung des deutschen Gesetzgebers der Kennzahlen auf relevante Einrichtungsart
- Unsicherheiten insbesondere bei Unternehmen, die mit Chemikalien umgehen und Konzern-IT
- Regulierung von Grenzüberschreitenden Sachverhalten noch detaillierter regelbar

Fragen?

Über Julian Monschke

Julian Monschke
Rechtsanwalt
Associated Partner

+49 69 971477179
julian.monschke@noerr.com

Julian Monschke berät zu Rechtsfragen des Informations-, IT- und Cybersicherheitsrechts sowie des IT- und Datenschutzrechts. Als Mitglied der Cyber Risks Group berät er regelmäßig bei grenzüberschreitenden Cybervorfällen sowie präventiv zu Fragen des BSIG, der KRITIS-VO und der NIS2-Richtlinie sowie weiteren regulatorischen Anforderungen. Seine Tätigkeit umfasst die Vertragsgestaltung und -verhandlung bei allen Formen der Überlassung von Soft- und Hardware. Ein Schwerpunkt von Herrn Monschke ist das Outsourcing von Unternehmen aus regulierten Branchen, insbesondere dem Finanzsektor. Im Bereich des Datenschutzrechts berät er bei der Erstellung rechtskonformer Dokumentationen von Verarbeitungsvorgängen - insbesondere bei der Einführung neuer Technologien (etwa KI).

Kompetenzen

- IT-Recht
- IT-Sicherheitsrecht
- Cybersicherheitsrecht
- Datenschutzrecht (DSGVO)
- Outsourcings

Pressestimmen

- Ones to Watch in Deutschland - Datensicherheit und Datenschutz: Handelsblatt/Best Lawyers 2024

Vielen Dank für Ihre Aufmerksamkeit!

Wichtiger Hinweis: Diese Präsentation stellt keine Rechtsberatung dar und ersetzt nicht die Beratung im konkreten Einzelfall. Für die Vollständigkeit und Richtigkeit wird keine Haftung übernommen. Sollten Sie zu den adressierten Themen Fragen oder Gesprächsbedarf haben, wenden Sie sich gerne an einen der Referenten oder einen anderen Ansprechpartner bei Noerr.