Rödl & Partner

EU-AUFLAGEN ZUR CYBERSICHERHEIT

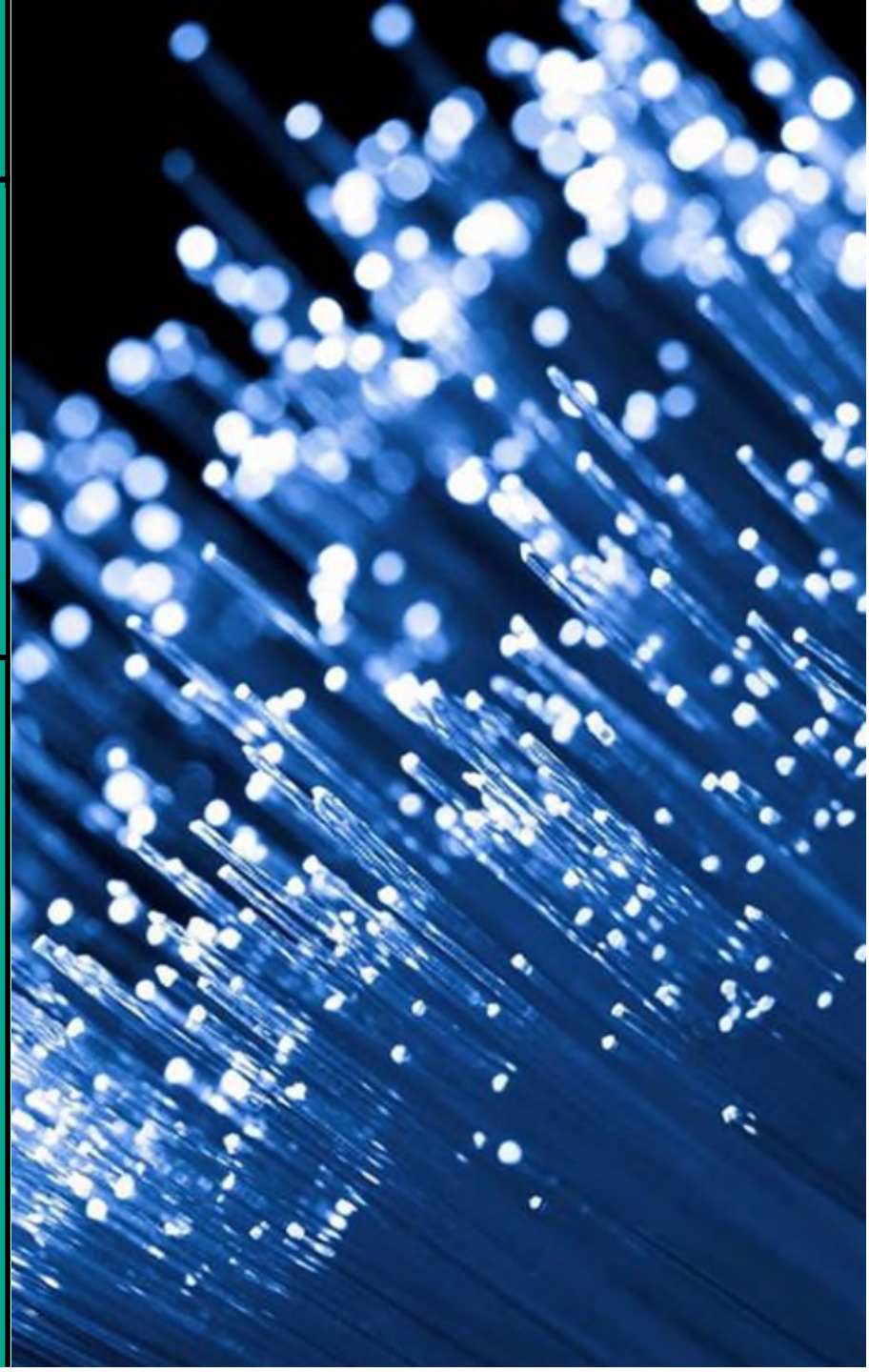
WER IST BETROFFEN UND WAS IST ZU TUN?

11. Kölner Vergabetage

Modul I: IT-Sicherheit, Cloud und neue EU-Auflagen zur Cybersicherheit – wie sicher sind Strategien, Praktiken und Richtlinien wirklich?

Johannes Marco Holz, Rechtsanwalt, FA IT-Recht

19. September 2023



AGENDA

I	**Vorstellung**
II	Zeitliche Einordung
III	Neuerungen der NIS-2 Richtlinie
IV	Anwendungsbereich
V	Risikomanagement
VI	Meldepflichten
VII	Sanktionen
VIII	Haftung von Leitungsorganen
IX	Ausblick
X	Fazit

I VORSTELLUNG DES DOZENTEN

JOHANNES MARCO HOLZ
Associate Partner
Rechtsanwalt

Fachanwalt für
Informationstechnologierecht
Zertifizierter Datenschutzbeauftragter
(GDDcert.EU)

T +49 911 9193 1511
M +49 176 6362 0371
johannes.holz@roedl.com

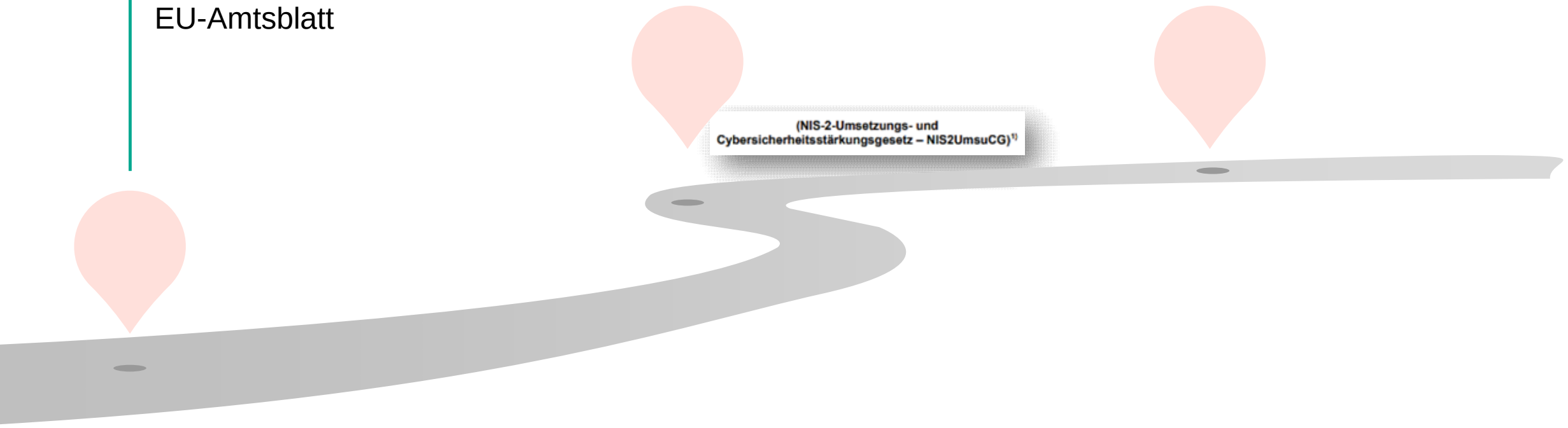
© Rödl & Partner

I ZEITLICHE EINORDNUNG

27.12.2022
Verkündung der NIS-2 Richtlinie im EU-Amtsblatt

03.07.2023
Aktueller Bearbeitungsstand Entwurf zur nationalen Umsetzung

17.10.2024
Ende der Umsetzungsfrist



© Rödl & Partner

II NEUERUNGEN DER NIS-2 RICHTLINIE

Hohes gemeinsames Cybersicherheitsniveau

- Schärfere Bußgeldvorschriften
- Meldepflichten bei Cyberattacken
- Stärkere Einbeziehung von Führungskräften
- Umfangreichere Risikomanagementmaßnahmen
- Mitgliedstaatlicher Peer Review
- Aufbau EU-Kooperationsgruppe
- Europäische Schwachstellendatenbank
- Aufstellung von CSIRTs
- Nationale Cybersicherheitsstrategien
- Neue Unterscheidung in wesentliche und wichtige Einrichtungen
- Bedeutende Ausweitung des Anwendungsbereichs

NIS-2 Richtlinie

© Rödl & Partner

III ANWENDUNGSBEREICH

Erfasst: öffentliche und private Einrichtungen

Mittlere Unternehmen:

- Anzahl Beschäftigter: 50 – 250
- Jahresumsatz 10 bis 50 Mio. EUR oder Jahresbilanz 10 bis 43 Mio. EUR

Große Unternehmen:

- Anzahl Beschäftigter: ab 250
- Jahresumsatz mehr als 50 Mio. EUR oder Jahresbilanz mehr als 43 Mio. EUR

Unabhängig von Größe:

- Anbieter öffentlicher elektronischer Kommunikationsnetze
- Einziger Anbieter in MS mit kritischer Tätigkeit
- Relevant für öffentliche Ordnung
- Systemrisiko
- Besondere Bedeutung der Einrichtung
- Einrichtung der öffentlichen Verwaltung
- Kritische Infrastruktur nach Resilienz-Richtlinie

In Anhang I oder Anhang II aufgeführte Einrichtung

© Rödl & Partner

III ANWENDUNGSBEREICH

Artikel 27

Register der Einrichtungen

(1) Die ENISA erstellt und pflegt ein Register der DNS-Diensteanbieter, TLD-Namenregister, Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter von verwalteten Diensten, Anbieter von verwalteten Sicherheitsdiensten sowie Anbieter von Online-Marktplätzen, Online-Suchmaschinen oder Plattformen für Dienste sozialer Netzwerke auf der Grundlage der Informationen, die sie von den zentralen Anlaufstellen im Einklang mit Artikel 4 erhalten hat. Auf Ersuchen ermöglicht die ENISA den zuständigen Behörden den Zugang zu diesem Register, wobei sie gegebenenfalls für den Schutz der Vertraulichkeit der Informationen sorgt.

(2) Die Mitgliedstaaten verlangen von den in Absatz 1 genannten Einrichtungen, dass sie bis zum 17. Januar 2025 den zuständigen Behörden folgende Angaben übermitteln:

a) Name der Einrichtung,

b) gegebenenfalls, einschlägiger Sektor, Teilsektor und Art der Einrichtung gemäß Anhang I oder II,

c) Anschrift der Hauptniederlassung der Einrichtung und ihrer sonstigen Niederlassungen in der Union oder, falls sie nicht in der Union niedergelassen ist, Anschrift ihres nach Artikel 26 Absatz 3 benannten Vertreters,

d) aktuelle Kontaktdaten, einschließlich E-Mail-Adressen und Telefonnummern der Einrichtung und gegebenenfalls ihres gemäß Artikel 26 Absatz 3 benannten Vertreters,

e) die Mitgliedstaaten, in denen die Einrichtung Dienste erbringt, und

f) die IP-Adressbereiche der Einrichtung.

© Rödl & Partner

III ANWENDUNGSBEREICH

Artikel 28

Datenbank der Domänennamen-Registrierungsdaten

(1) Um einen Beitrag zur Sicherheit, Stabilität und Resilienz des Domänennamensystems zu leisten, verpflichten die Mitgliedstaaten, dass die TLD-Namenregister und die Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, genaue und vollständige Domänennamen-Registrierungsdaten in einer eigenen Datenbank im Einklang mit dem Datenschutzrecht der Union in Bezug auf personenbezogene Daten mit der gebotenen Sorgfalt sammeln und pflegen.

(2) Für die Zwecke des Absatzes 1 schreiben die Mitgliedstaaten vor, dass die Datenbank der Domänennamen-Registrierungsdaten die erforderlichen Angaben enthält, anhand derer die Inhaber der Domänennamen und die Kontaktstellen, die die Domänennamen im Rahmen der TLD verwalten, identifiziert und kontaktiert werden können. Diese Informationen müssen Folgendes umfassen:

a) den Domänennamen;

b) das Datum der Registrierung;

c) den Namen des Domäneninhabers, seine E-Mail-Adresse und Telefonnummer;

d) die Kontakt-E-Mail-Adresse und die Telefonnummer der Anlaufstelle, die den Domänennamen verwaltet, falls diese sich von denen des Domäneninhabers unterscheiden.

© Rödl & Partner

III ANWENDUNGSBEREICH

Anhang I:
Sektoren mit hoher Kritikalität

z.B. Betreiber eines Stromnetzes, Fluglinien, Kreditinstitute, pharmazeutische Hersteller, Trinkwasserversorgung, Abwasserentsorgung, öffentliche Verwaltung

Anhang II:
Sonstige kritische Sektoren

z.B. Postdienstleistungen, Unternehmen der Abfallwirtschaft, Produktion chemischer Stoffe, Produktion von Lebensmitteln, Hersteller von Kfz und Zulieferer, Online-Marktplätze

© Rödl & Partner

III ANWENDUNGSBEREICH

Unterscheidung der Einrichtungen

Wesentliche Einrichtungen

- **Einrichtung nach Anhang I und große Unternehmen**
- **Qualifizierte Vertrauensdienstleister und Domänennamensregister**
- **Öffentliche elektronische Kommunikationsnetze**
- **Öffentliche Verwaltung**

Wichtige Einrichtungen

- **Einrichtung nach Anhang I oder Anhang II und keine wesentliche Einrichtung**

© Rödl & Partner

IV RISIKOMANAGEMENT

Analyse der vorhandenen Struktur

Konkrete Maßnahmen

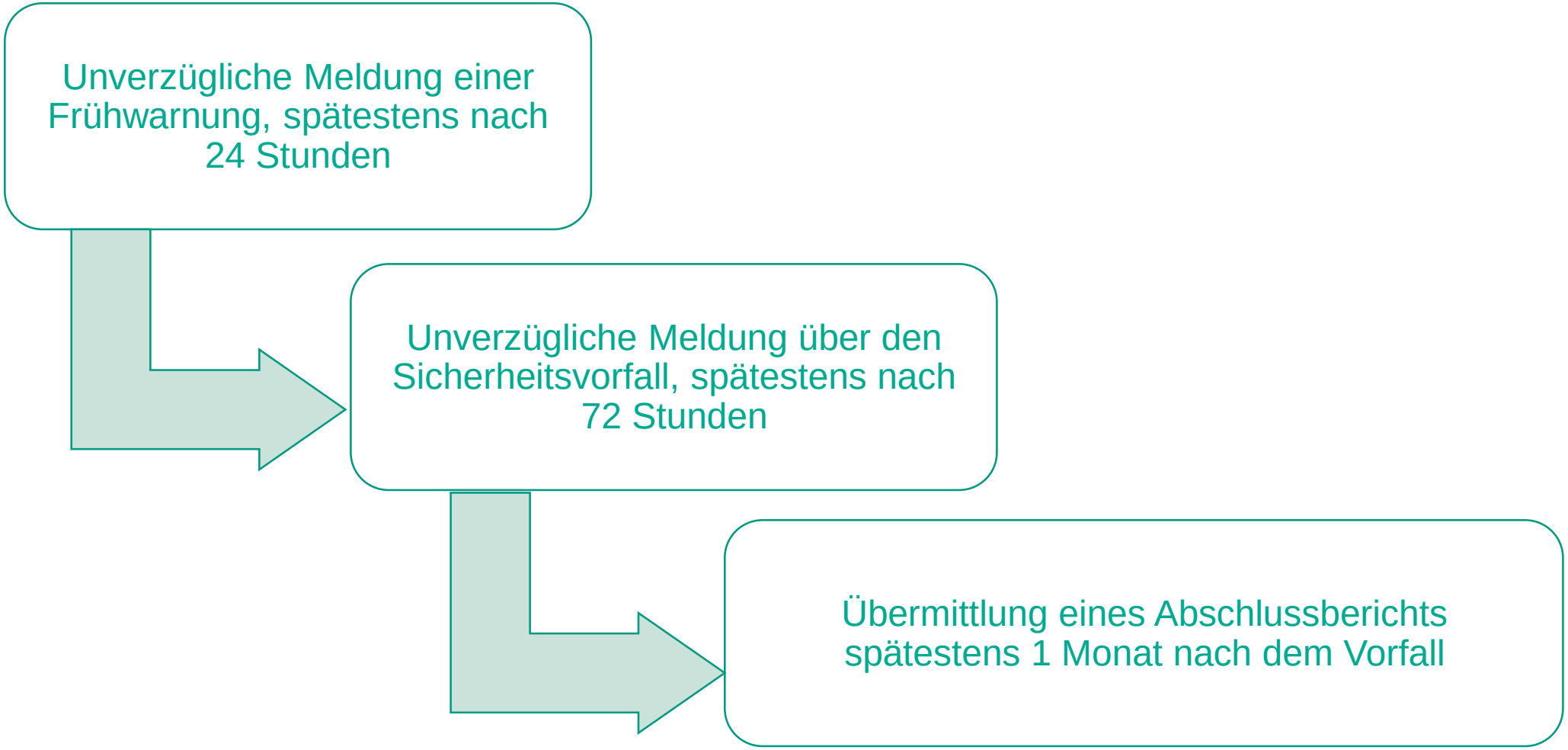
Schutz vor digitalen und physischen Gefahren mit Mindestmaßnahmen:

- Konzepte in Bezug auf Risikoanalyse
- Bewältigung von Sicherheitsvorfällen
- Aufrechterhaltung des Betriebs z.B. durch Backup-Management
- Sicherheit der Lieferkette
- Schulungen im Bereich Cybersicherheit
- Verschlüsselung und Authentifizierung

© Rödl & Partner

V MELDEPFLICHTEN

Vorgehensweise bei einem erheblichen Sicherheitsvorfall



© Rödl & Partner

VI SANKTIONEN

Grundsatz: Behördliche Maßnahmen müssen wirksam, verhältnismäßig und abschreckend sein

Wesentliche Einrichtungen

- **Vor-Ort-Kontrollen**
- **Sicherheitsprüfungen und Ad-hoc-Prüfungen**
- **Sicherheitsscans**
- **Auskunftsverlangen und Dokumentenvorlage**
- **Aussprechen von Warnungen**
- **Verbindliche Anweisungen**
- **Information der Öffentlichkeit**
- **Verhängung einer Geldbuße**

© Rödl & Partner

VI SANKTIONEN

Grundsatz: Behördliche Maßnahmen müssen wirksam, verhältnismäßig und abschreckend sein

Wichtige Einrichtungen

- Vor-Ort-Kontrollen
- Sicherheitsprüfungen
- Sicherheitsscans
- Auskunftsverlangen und Dokumentenvorlage
- Aussprechen von Warnungen
- Verbindliche Anweisungen
- Information der Öffentlichkeit
- Verhängung einer Geldbuße

© Rödl & Partner

VI SANKTIONEN

Zusätzliche Geldbußen möglich bei Verstößen gegen Aufsichts- oder Durchsetzungsmaßnahmen oder Meldepflichten

Wesentliche Einrichtungen

Höchstbetrag von 10 Mio. EUR

oder

2% des weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes

Wichtige Einrichtungen

Höchstbetrag von 7 Mio. EUR

oder

1,4% des weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes

© Rödl & Partner

VII HAFTUNG VON LEITUNGSORGANEN

Überwachung der Umsetzung der Risikomanagementmaßnahmen

Teilnahme an Schulungen

Persönliche Verantwortlichkeit für Verstöße

Persönliche Haftung bei Verstößen gegen die NIS-2 Richtlinie

Nur bei wesentlichen Einrichtungen:

Vorübergehende Untersagung Leitungsaufgaben auszuüben

© Rödl & Partner

VII HAFTUNG VON LEITUNGSORGANEN

Artikel 20

Governance

(1) Die Mitgliedstaaten stellen sicher, dass die Leitungsorgane wesentlicher und wichtiger Einrichtungen die von diesen Einrichtungen zur Einhaltung von Artikel 21 ergriffenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit billigen, ihre Umsetzung überwachen und für Verstöße gegen diesen Artikel durch die betreffenden Einrichtungen verantwortlich gemacht werden können.

Die Anwendung dieses Absatzes lässt die nationalen Rechtsvorschriften in Bezug auf die für die öffentlichen Einrichtungen geltenden Haftungsregelungen sowie die Haftung von öffentlichen Bediensteten und gewählten oder ernannten Amtsträgern unberührt.

(2) Die Mitgliedstaaten stellen sicher, dass die Mitglieder der Leitungsorgane wesentlicher und wichtiger Einrichtungen an Schulungen teilnehmen müssen, und fordern wesentliche und wichtige Einrichtungen auf, allen Mitarbeitern regelmäßig entsprechende Schulungen anzubieten, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben.

© Rödl & Partner

VII HAFTUNG VON LEITUNGSORGANEN

§ 38

Billigungs-, Überwachungs- und Schulungspflicht für Geschäftsleiter besonders wichtiger Einrichtungen und wichtiger Einrichtungen

(1) Geschäftsleiter besonders wichtiger Einrichtungen und wichtiger Einrichtungen sind verpflichtet, die von diesen Einrichtungen zur Einhaltung von § 30 ergriffenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit zu billigen und ihre Umsetzung zu überwachen. Die Beauftragung eines Dritten zu Erfüllung der Verpflichtungen nach Satz 1 ist nicht zulässig.

(2) Geschäftsleiter, welche ihre Pflichten nach Absatz 1 verletzen, haften der Einrichtung für den entstandenen Schaden. Satz 1 gilt nicht für Geschäftsleiter besonders wichtiger Einrichtungen des Teilsektors Zentralregierung des Sektors öffentliche Verwaltung.

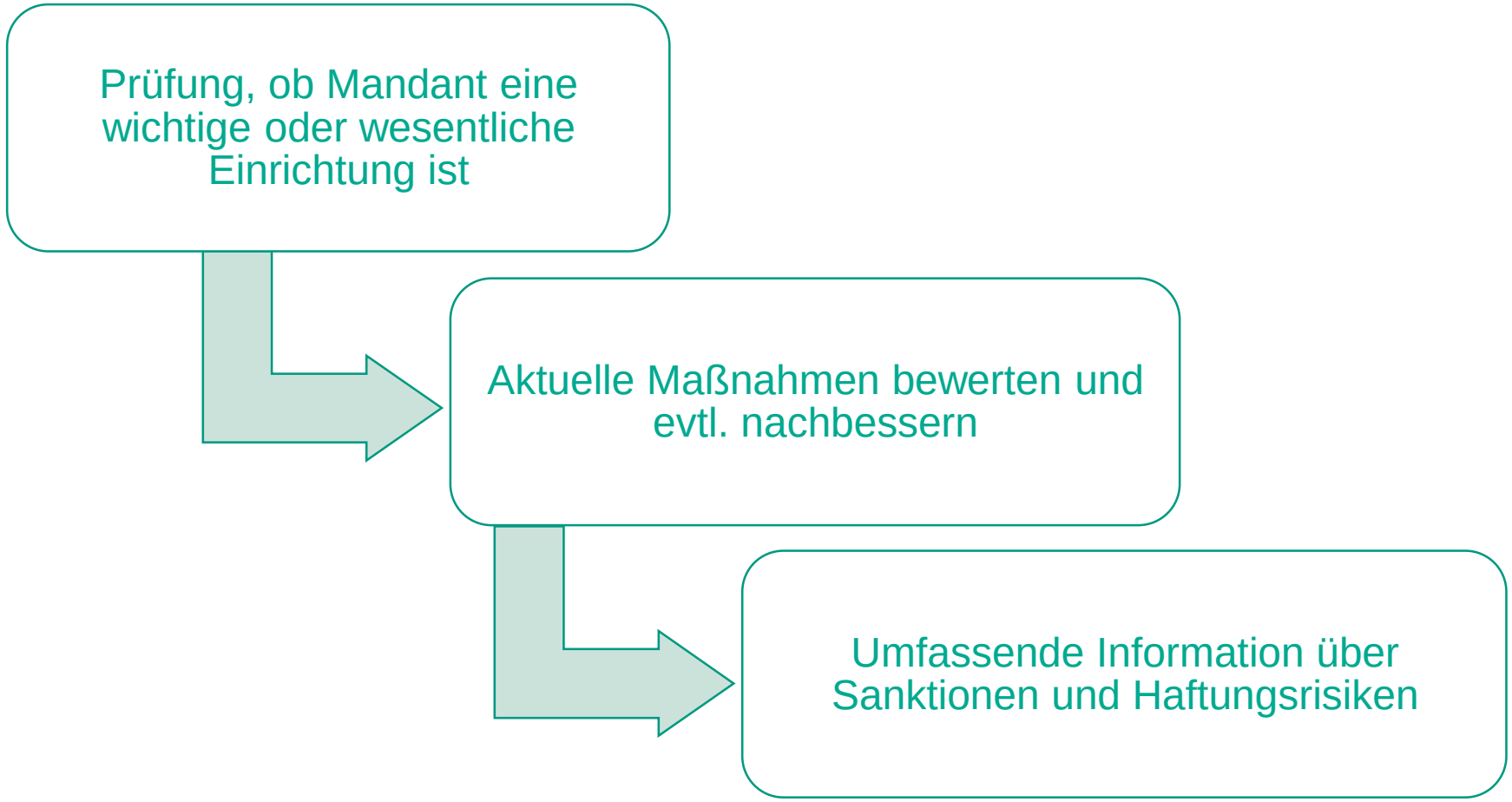
(3) Ein Verzicht der Einrichtung auf Ersatzansprüche nach Absatz 2 oder ein Vergleich der Einrichtung über diese Ansprüche ist unwirksam. Dies gilt nicht, wenn der Ersatzpflichtige zahlungsunfähig ist und sich zur Abwendung des Insolvenzverfahrens mit seinen Gläubigern vergleicht oder wenn die Ersatzpflicht in einem Insolvenzplan geregelt wird.

(4) Die Geschäftsleiter von besonders wichtigen Einrichtungen und wichtigen Einrichtungen müssen und deren Mitarbeiter sollen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Risikomanagementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben.

© Rödl & Partner

VIII AUSBLICK

Unsere Beratung zur NIS-2-Richtlinie



© Rödl & Partner

Rödl & Partner

EU-AUFLAGEN ZUR CYBERSICHERHEIT

WER IST BETROFFEN UND WAS IST ZU TUN?

11. Kölner Vergabetage

Modul I: IT-Sicherheit, Cloud und neue EU-Auflagen zur Cybersicherheit – wie sicher sind Strategien, Praktiken und Richtlinien wirklich?

Johannes Marco Holz, Rechtsanwalt, FA IT-Recht

19. September 2023