Deloitte. Legal

JANK WEILER OPERENYI RECHTSANWÄLTE

NIS2-Richtlinie

Die wichtigsten rechtlichen Aspekte von NIS2

RA Hon.-Prof. (FH) Mag. Sascha Jung, LL.M. LL.M.

Die NIS2-Richtlinie / Entwurf NIS-G 2024

Allgemeine Informationen

Was ist NIS2?

- NIS2 (Network and Information Security 2) ist eine EU-Richtlinie
- NIS2 zielt darauf ab, Sicherheit der Informations- und Kommunikationstechnologie (IKT) in Europa zu stärken

Adressaten

- NIS2 gilt für Unternehmen in wesentlichen und wichtigen Sektoren ab mittlerer Unternehmensgröße und Betreiber digitaler Infrastruktur in EU-Mitgliedsstaaten, Island, Lichtenstein, Norwegen
- Diese müssen Sicherheitsvorkehrungen treffen, um Cyberbedrohungen zu erkennen, ihnen entgegenzuwirken und darauf zu reagieren

Inhalt

- Vorschriften zur Cyber Security, z.B. Risikomanagementansatz, Lieferketten und Partnerunternehmen
- Bestimmungen zur Meldung von Sicherheitsvorfällen sowie zur Zusammenarbeit und Koordination zwischen den Mitgliedstaaten der EU
- Sanktionen

Ziel

- die Fähigkeit der EU-Mitgliedstaaten stärken, auf Cyberbedrohungen und -vorfälle zu reagieren
- die Integrität des digitalen Binnenmarkts schützen
- hohes gemeinsames Cybersicherheitsniveau in der EU
- Ablösung der NIS-1 (Inkrafttreten: 08.08.2016)

Umsetzung

- NIS2 ist am 16.01.2024 in Kraft getreten
- wird bis 17.10.2024 in nationales Recht umgesetzt. Zu dem Stichdatum müssen betroffene Unternehmen NIS2-konform sein
- Seit Anfang April 2024 ist der Begutachtungsentwurf des NIS-G 2024 im RIS veröffentlicht, die Begutachtungsfrist endet am 1.5.2024

Die NIS2-Richtlinie / Entwurf NIS-G 2024 (§ 24)

Adressaten der NIS2-Richtlinie bzw. des NIS-G sind Unternehmen in wesentlichen und wichtigen Sektoren, welche mindestens mittlerer Größe klassifiziert sind und Betreiber digitaler Infrastruktur

Wesentliche Einrichtungen

Zu den wesentlichen Einrichtungen gehören vor allem KRITIS-Unternehmen, also Betriebe mit **wichtiger Bedeutung für das staatliche Gemeinwesen, deren Ausfall gravierende Folgen** hätte. Dazu gehören Unternehmen mit einer Tätigkeit in einem der folgenden Sektoren:

- Energie
- Verkehr
- Bankwesen
- Finanzmarktinfrastrukturen
- Gesundheitswesen
- Trinkwasser
- Abwasser
- Digitale Infrastruktur
- Verwaltung von IKT-Diensten (b2b)
- Öffentliche Verwaltung
- Weltraum

Wichtige Einrichtungen

Zu den wichtigen Einrichtungen werden Unternehmen mit Tätigkeiten in folgenden Sektoren gezählt:

- Post- und Kurierdienste
- Abfallbewirtschaftung
- Produktion, Herstellung und Handel mit chemischen Stoffen
- Produktion, Verarbeitung und Vertrieb von Lebensmitteln
- Verarbeitendes Gewerbe / Herstellung von Waren
  - Medizinprodukte und In-vitro-Diagnostika
  - Datenverarbeitungsgeräte, elektronischen und optischen Erzeugnissen
  - Elektrischen Ausrüstungen
  - Maschinenbau
  - Kraftwagen und -teilen
  - Sonstiger Fahrzeugbau
- Anbieter digitaler Dienste
- Forschung

Die NIS2-Richtlinie / Entwurf NIS-G 2024 (§ 25)

Adressaten der NIS2-Richtlinie bwz. des NIS-G sind gemäß der Size-Cap-Rule Unternehmen in wesentlichen und wichtigen Sektoren, welche mindestens mittlerer Größe klassifiziert sind und Betreiber digitaler Infrastruktur

	Beschäftigte (VZÄ)		Jahresumsatz		Jahresbilanzsumme
Kleines Unternehmen (KU)	weniger als 50	**Alternativ**	weniger als EUR 10 Mio	**oder**	weniger als EUR 10 Mio
Mittleres Unternehmen (MU)	zumindest 50 und weniger als 250	**Alternativ**	mehr als EUR 10 Mio	**und**	mehr als EUR 10 Mio
			und nicht bereits ein großes Unternehmen		
Großes Unternehmen (GU)	zumindest 250	**Alternativ**	mehr als EUR 50 Mio	**und**	mehr als EUR 43 Mio

Mittlere und große Unternehmen in den wesentlichen und wichtigen Sektoren fallen gemäß der Size-Cap-Rule unter NIS2

Die NIS2-Richtlinie / Entwurf NIS-G 2024 (§§ 24, 26)

Mögliche Adressaten der NIS2-Richtlinie bzw. des NIS-G sind bei bestimmten Kriterien auch kleine Unternehmen

	Betroffen durch Sektor	**Betroffen durch Lieferkette**
Unternehmen unabhängig ihrer Unternehmensgröße	• Qualifizierter Vertrauensdienstanbieter • Anbieter öffentlicher elektronischer Kommunikationsnetze oder Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste • TLD-Namenregister und DNS-Diensteanbieter, ausgenommen Betreiber von Root-Namenservern • Unternehmen, die alleiniger Anbieter eines Service in einem Mitgliedstaat sind, das essenziell für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Aktivitäten ist.	• Dienstleister und Lieferanten von betroffenen Unternehmen

Wichtig: auch kleine Unternehmen können durch den Sektor oder die Lieferkette von NIS2 betroffen sein

Inhalt der NIS2-Richtlinie / des Entwurfs NIS-G 2024

Betroffene Unternehmen müssen die folgenden Cybersicherheitsanforderungen erfüllen

Registrierung

Risikomanagementmaßnahmen

Meldung von Sicherheitsvorfällen gegenüber Behörde / CSIRT; Unterrichtung von Kunden

Meldepflichten durch die NIS2-Richtlinie / Entwurf NIS-G 2024 (§ 34)

NIS 2 verschärft die Meldepflichten von erheblichen Sicherheitsvorfällen bei wesentlichen und wichtigen Einrichtungen gegenüber CSIRT / Behörde

Was ist ein erheblicher Sicherheitsvorfall?

Sicherheitsvorfall, der

- **schwerwiegende** Betriebsstörungen der Dienste / finanzielle Verluste für die Einrichtung verursacht hat / verursachen kann;

oder

- andere natürliche / juristische Personen durch **erhebliche** materielle / immaterielle Schäden beeinträchtigt hat / beeinträchtigen kann.

1 **Frühwarnung**
(unverzüglich aber max. 24 h nach Kenntnis)

2 **Meldung**
(unverzüglich aber max. 72 h nach Kenntnis)

3 **Zwischenbericht**
(jederzeit auf Ersuchen)

4 **Abschlussbericht**
(1 Monat nach Meldung)

4 **Andauernder Vorfall: Fortschrittsbericht**
(1 Monat nach Meldung;)

5 **Abschlussbericht**
(1 Monat nach Bewältigung des Vorfalls

Unterrichtungspflichten gegenüber Kunden (§ 34, 39)

NIS 2 verschärft auch die Pflicht ggf. die Kunden über den Sicherheitsvorfall / die Cyberbedrohung zu informieren

	Erheblicher Sicherheitsvorfall	**Erhebliche Cyberbedrohung**
Wen unterrichten?	Empfänger von Einrichtungsdiensten	Potenziell betroffene Empfänger von Einrichtungsdiensten
Über was?	erheblicher Sicherheitsvorfall, der Diensterbringung beeinträchtigen könnte	• (Abhilfe) Maßnahmen, die sie ergreifen können • ggf. erhebliche Cyberbedrohung
Wann?	unverzüglich	unverzüglich

Sanktionen bei Verstoß gegen die NIS2-Richtlinie / Entwurf NIS-G 2024 (§§ 44 ff.)

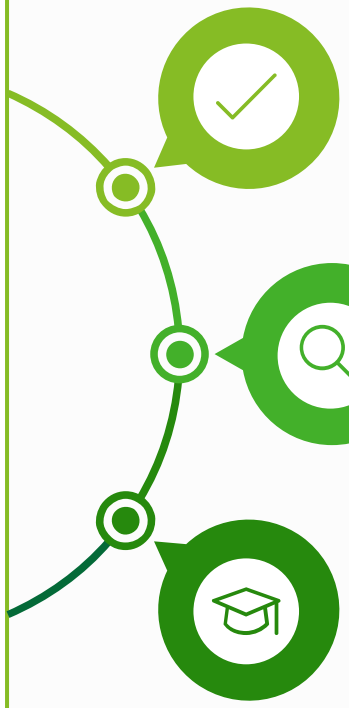
Verhängte Sanktionen hängen von der Kritikalität der Einrichtung ab

	Wesentliche Einrichtung	Wichtige Einrichtung
Aufsicht	ex ante, ex post	ex post
Geldbußen	für Verstöße gegen Risikomanagementmaßnahmen oder Meldepflichten maximal mindestens 10 Mio. € oder 2 % des weltweiten Vorjahresumsatzes	7 Mio. € oder 1,4 % des weltweiten Vorjahresumsatzes je nachdem, welcher Betrag höher ist
Weitere Sanktionen	Verhängung zusätzlicher Sanktionen für denselben Verstoß möglich (z.B. Warnung über Verstoß der Einrichtung gegen NIS2-Umsetzungsgesetz)	

Cybersicherheit als Governance-Aufgabe der Geschäftsleitung (§3 31, 32)

Die Geschäftsführung bzw. der Vorstand wird in Zukunft viel mehr in die Pflicht genommen

Zu den Pflichten des Vorstands und der Geschäftsführer gehört:



Billigung der getroffenen Risikomanagementmaßnahmen

Überwachung ihrer Umsetzung

Teilnahme an **Schulungen**

Konsequenzen bei Nichtbeachtung:

Persönliche Haftung bei Pflichtverletzung:
Haftung gegenüber der Einrichtung für entstandenen Schaden mit Privatvermögen

In Extremfällen kann bei wesentlichen Einrichtungen eine vorübergehende **Untersagung der Wahrnehmung der Leitungsaufgaben möglich!**

NIS2-Richtlinie / Entwurf NIS-G 2024 und DSGVO (§§ 21, 42)

Die beiden Rechtsgrundlagen arbeiten nicht gegeneinander, sondern sind als Konvergenz zu sehen

Die Vorgaben der DSGVO bleiben von NIS 2 unberührt. Mit der Umsetzung von NI 2 gehen notwendigerweise **datenschutzrechtliche Handlungspflichten** einher, insbesondere:

- Anpassung des **Verarbeitungsverzeichnisses** und der **Datenschutzinformationen**
- Durchführung von **Datenschutzfolgenabschätzungen**
- Anpassung der **TOMs**

Sofern Sicherheitsvorfälle auch die Verletzung **personenbezogener Daten** umfassen:

- Muss die NIS2 Behörde im Fall einer datenschutzrechtlichen Meldepflicht **die DSB darüber informieren**
- Müssen zusätzlich **Data-Breach-Meldungen an die DSB** erfolgen
- Gilt das **Sanktionsregime der DSGVO und der DSB** (Strafrahmen bis zu EUR 10/20 Mio oder 2/4% des weltweiten Jahresumsatzes)
- Kann zeitnah eine **nachträgliche Datenschutzüberprüfung** durch die DSB erfolgen

NIS2 ist stets im Zusammenhang mit der DSGVO zu betrachten.
Eine vollständige Umsetzung von NIS2 bedingt konsequenterweise eine vollständige DSGVO-Implementierung.

Wir stehen Ihnen gerne als Ansprechpartner zur Verfügung

Ihr Deloitte Legal Team

Sascha Jung
Partner - Tax und Legal

+43 676 6269912
s.jung@jankweiler.at

Christian Kern
Senior Manager – Tax und Legal

+43 660 666 0046
c.kern@jankweiler.at