SNV
standards connect
the world

Seminar NIS-2-Richtlinie Rechtliche Aspekte

Martin Eckert, MME Legal Tax Compliance, Legal Partner

Zürich, 03. Juli 2024

Schweizerische Normen-Vereinigung (SNV)
Association Suisse de Normalisation (SNV)
Swiss Association for Standardization (SNV)

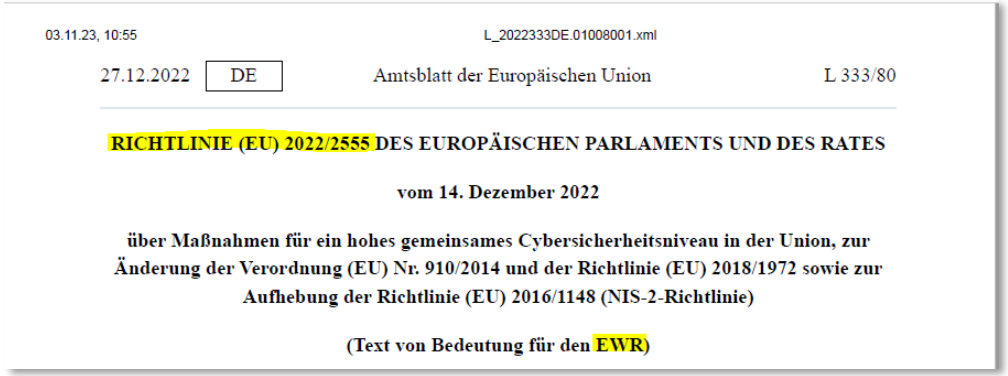
Sulzerallee 70, Postfach
CH-8404 Winterthur/Switzerland, T +41 52 224 54 54
info@snv.ch, www.snv.ch

Member
International Organization for Standardization (ISO)
Comité Européen de Normalisation (CEN)

Inhaltsverzeichnis Vortrag Dr. Martin Eckert

1. Rechtliche Einordnung der NIS-2-Richtlinie

- NIS-2: Weiterentwicklung der Richtlinie (EU) 2016/1148



03.11.23, 10:55 L_2022333DE.01008001.xml

27.12.2022 DE Amtsblatt der Europäischen Union L 333/80

RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 14. Dezember 2022

über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)

(Text von Bedeutung für den EWR)

- Adressaten (Art. 46): EU- und EWR-Mitgliedstaaten; ENISA (EU-Behörde)
- Richtlinie ist Non-self executing (keine Verordnung)
- Muss-Vorschriften / Kann-Vorschriften für Mitgliedstaaten
- Aufhebung von Vorschriften (insbesondere Richtlinie (EU) 2016/1148)
- NIS: „Netz- und Informationssystem“

2. Nationale Umsetzung – Beispiel Deutschland

- Federführend ist das Bundesministerium des Innern und für Heimat (+ BSI)

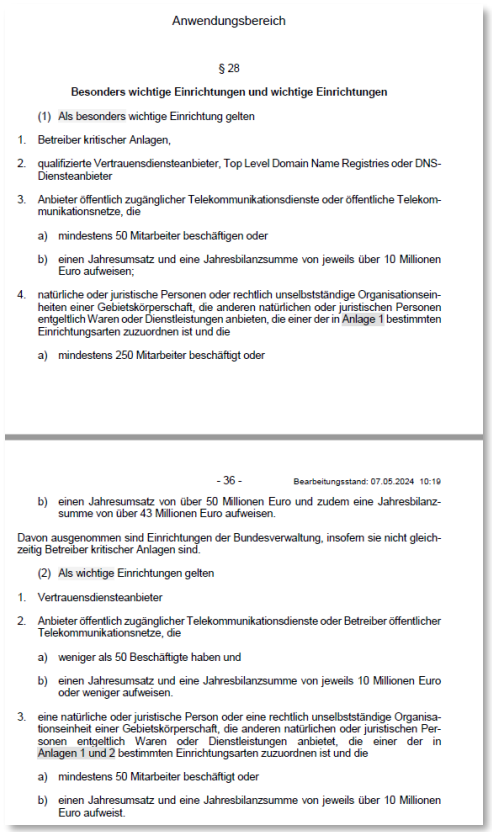
https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/nis2umsucg.html

3. Zeitachse: Bis wann muss ich Pflichten umsetzen?

- NIS-2-Richtlinie in Kraft seit Veröffentlichung 27.12.2022
- Umsetzung durch Mitgliedstaaten bis 17. Oktober 2024
- Deutschland: Inkrafttreten **NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz** für 1. Oktober 2024 geplant
- Übergangsfristen für Umsetzung durch Private? Nein, aber:

(3) Das Bundesamt kann, neben der nach § 39 für Betreiber einer kritischen Anlage bestimmten Frist, auch gegenüber anderen besonders wichtigen Einrichtungen frühestens drei Jahre nach Inkrafttreten dieses Gesetzes die Vorlage von Nachweisen über die Erfüllung einzelner oder aller Anforderungen nach den §§ 30, 31 und 32 anordnen. Soweit das Bundesamt von seinem Recht nach Absatz 1 Gebrauch gemacht hat, kann es hierbei auch die Übermittlung der Ergebnisse der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel sowie die Vorlage der Dokumentation, die der Überprüfung zugrunde gelegt wurde, verlangen. Es kann bei Sicherheitsmängeln die Vorlage eines geeigneten Mängelbeseitigungsplans im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder der sonst zuständigen Aufsichtsbehörde verlangen. Das Bundesamt kann die Vorlage eines geeigneten Nachweises über die erfolgte Mängelbeseitigung verlangen.

4. Anwendungsbereich – komplexe Regelung (Art. 2)



Anwendungsbereich

§ 28

Besonders wichtige Einrichtungen und wichtige Einrichtungen

(1) Als besonders wichtige Einrichtung gelten

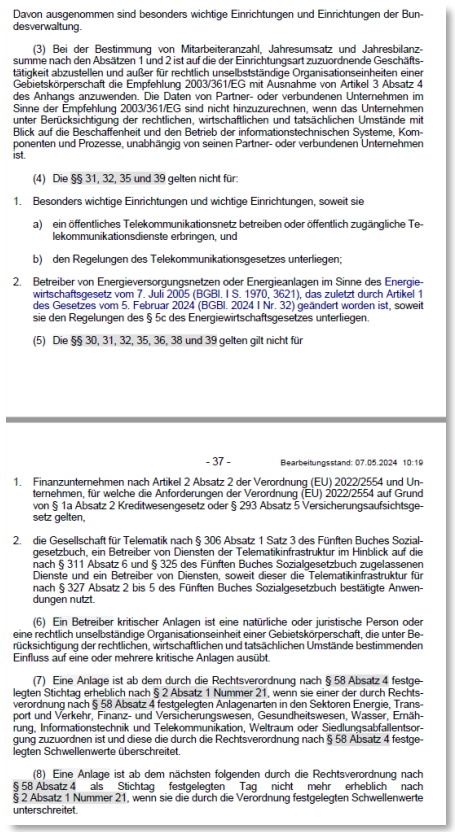
1. Betreiber kritischer Anlagen,
2. qualifizierte Vertrauensdiensteanbieter, Top Level Domain Name Registries oder DNS-Diensteanbieter
3. Anbieter öffentlich zugänglicher Telekommunikationsdienste oder öffentliche Telekommunikationsnetze, die
   a) mindestens 50 Mitarbeiter beschäftigen oder
   b) einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro aufweisen;
4. natürliche oder juristische Personen oder rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft, die anderen natürlichen oder juristischen Personen entgeltlich Waren oder Dienstleistungen anbieten, die einer der in Anlage 1 bestimmten Einrichtungsarten zuzuordnen ist und die
   a) mindestens 250 Mitarbeiter beschäftigt oder

   b) einen Jahresumsatz von über 50 Millionen Euro und zudem eine Jahresbilanzsumme von über 43 Millionen Euro aufweisen.

Davon ausgenommen sind Einrichtungen der Bundesverwaltung, insofern sie nicht gleichzeitig Betreiber kritischer Anlagen sind.

(2) Als wichtige Einrichtungen gelten

1. Vertrauensdiensteanbieter
2. Anbieter öffentlich zugänglicher Telekommunikationsdienste oder Betreiber öffentlicher Telekommunikationsnetze, die
   a) weniger als 50 Beschäftigte haben und
   b) einen Jahresumsatz und eine Jahresbilanzsumme von jeweils 10 Millionen Euro oder weniger aufweisen.
3. eine natürliche oder juristische Person oder eine rechtlich unselbstständige Organisationseinheit einer Gebietskörperschaft, die anderen natürlichen oder juristischen Personen entgeltlich Waren oder Dienstleistungen anbietet, die einer der in Anlagen 1 und 2 bestimmten Einrichtungsarten zuzuordnen ist und die
   a) mindestens 50 Mitarbeiter beschäftigt oder
   b) einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro aufweist.



Davon ausgenommen sind besonders wichtige Einrichtungen und Einrichtungen der Bundesverwaltung.

(3) Bei der Bestimmung von Mitarbeiteranzahl, Jahresumsatz und Jahresbilanzsumme nach den Absätzen 1 und 2 ist auf die der Einrichtungsart zuzuordnende Geschäftstätigkeit abzustellen und außer für rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft die Empfehlung 2003/361/EG mit Ausnahme von Artikel 3 Absatz 4 des Anhangs anzuwenden. Die Daten von Partner- oder verbundenen Unternehmen im Sinne der Empfehlung 2003/361/EG sind nicht hinzuzurechnen, wenn das Unternehmen unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände mit Blick auf die Beschaffenheit und den Betrieb der informationstechnischen Systeme, Komponenten und Prozesse, unabhängig von seinen Partner- oder verbundenen Unternehmen ist.

(4) Die §§ 31, 32, 35 und 39 gelten nicht für:

1. Besonders wichtige Einrichtungen und wichtige Einrichtungen, soweit sie
   a) ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen, und
   b) den Regelungen des Telekommunikationsgesetzes unterliegen;
2. Betreiber von Energieversorgungsnetzen oder Energieanlagen im Sinne des Energiewirtschaftsgesetz vom 7. Juli 2005 (BGBl. I S. 1970, 3621), das zuletzt durch Artikel 1 des Gesetzes vom 5. Februar 2024 (BGBl. 2024 I Nr. 32) geändert worden ist, soweit sie den Regelungen des § 5c des Energiewirtschaftsgesetzes unterliegen.

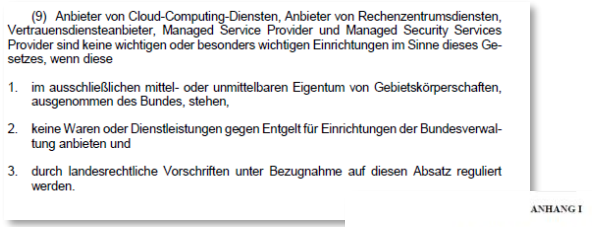
(5) Die §§ 30, 31, 32, 35, 36, 38 und 39 gelten gilt nicht für

1. Finanzunternehmen nach Artikel 2 Absatz 2 der Verordnung (EU) 2022/2554 und Unternehmen, für welche die Anforderungen der Verordnung (EU) 2022/2554 auf Grund von § 1a Absatz 2 Kreditwesengesetz oder § 293 Absatz 5 Versicherungsaufsichtsgesetz gelten,
2. die Gesellschaft für Telematik nach § 306 Absatz 1 Satz 3 des Fünften Buches Sozialgesetzbuch, ein Betreiber von Diensten der Telematikinfrastruktur im Hinblick auf die nach § 311 Absatz 6 und § 325 des Fünften Buches Sozialgesetzbuch zugelassenen Dienste und ein Betreiber von Diensten, soweit dieser die Telematikinfrastruktur für nach § 327 Absatz 2 bis 5 des Fünften Buches Sozialgesetzbuch bestätigte Anwendungen nutzt.

(6) Ein Betreiber kritischer Anlagen ist eine natürliche oder juristische Person oder eine rechtlich unselbständige Organisationseinheit einer Gebietskörperschaft, die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss auf eine oder mehrere kritische Anlagen ausübt.

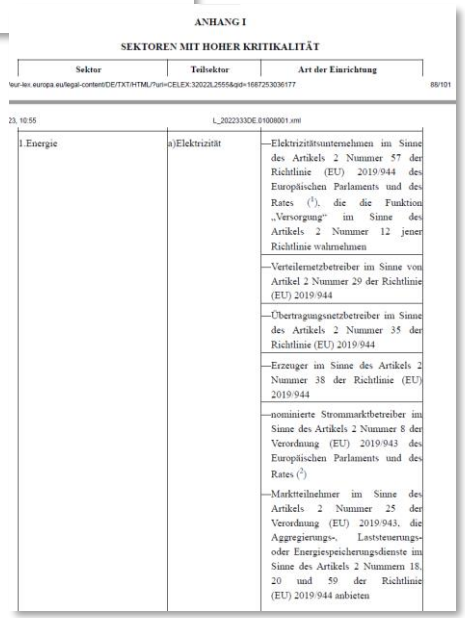
(7) Eine Anlage ist ab dem durch die Rechtsverordnung nach § 58 Absatz 4 festgelegten Stichtag erheblich nach § 2 Absatz 1 Nummer 21, wenn sie einer der durch Rechtsverordnung nach § 58 Absatz 4 festgelegten Anlagenarten in den Sektoren Energie, Transport und Verkehr, Finanz- und Versicherungswesen, Gesundheitswesen, Wasser, Ernährung, Informationstechnik und Telekommunikation, Weltraum oder Siedlungsabfallentsorgung zuzuordnen ist und diese die durch die Rechtsverordnung nach § 58 Absatz 4 festgelegten Schwellenwerte überschreitet.

(8) Eine Anlage ist ab dem nächsten folgenden durch die Rechtsverordnung nach § 58 Absatz 4 als Stichtag festgelegten Tag nicht mehr erheblich nach § 2 Absatz 1 Nummer 21, wenn sie die durch die Verordnung festgelegten Schwellenwerte unterschreitet.



(9) Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Vertrauensdiensteanbieter, Managed Service Provider und Managed Security Services Provider sind keine wichtigen oder besonders wichtigen Einrichtungen im Sinne dieses Gesetzes, wenn diese

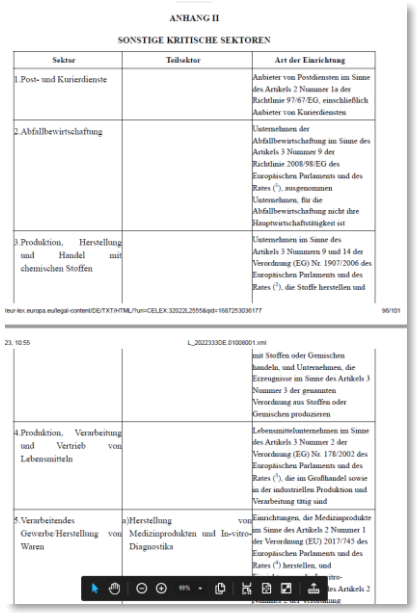
1. im ausschließlichen mittel- oder unmittelbaren Eigentum von Gebietskörperschaften, ausgenommen des Bundes, stehen,
2. keine Waren oder Dienstleistungen gegen Entgelt für Einrichtungen der Bundesverwaltung anbieten und
3. durch landesrechtliche Vorschriften unter Bezugnahme auf diesen Absatz reguliert werden.



ANHANG I

SEKTOREN MIT HOHER KRITIKALITÄT

Sektor	Teilsektor	Art der Einrichtung
1. Energie	a) Elektrizität	— Elektrizitätsunternehmen im Sinne des Artikels 2 Nummer 57 der Richtlinie (EU) 2019/944 des Europäischen Parlaments und des Rates (3), die die Funktion „Versorgung" im Sinne des Artikels 2 Nummer 12 jener Richtlinie wahrnehmen — Verteilernetzbetreiber im Sinne von Artikel 2 Nummer 29 der Richtlinie (EU) 2019/944 — Übertragungsnetzbetreiber im Sinne des Artikels 2 Nummer 35 der Richtlinie (EU) 2019/944 — Erzeuger im Sinne des Artikels 2 Nummer 38 der Richtlinie (EU) 2019/944 — nominierte Strommarktbetreiber im Sinne des Artikels 2 Nummer 8 der Verordnung (EU) 2019/943 des Europäischen Parlaments und des Rates (2) — Marktteilnehmer im Sinne des Artikels 2 Nummer 25 der Verordnung (EU) 2019/943, die Aggregierungs-, Laststeuerungs- oder Energiespeicherungsdienste im Sinne des Artikels 2 Nummern 18, 20 und 59 der Richtlinie (EU) 2019/944 anbieten



ANHANG II

SONSTIGE KRITISCHE SEKTOREN

Sektor	Teilsektor	Art der Einrichtung
1. Post- und Kurierdienste		Anbieter von Postdiensten im Sinne des Artikels 2 Nummer 1a der Richtlinie 97/67/EG, einschließlich Anbieter von Kurierdiensten
2. Abfallbewirtschaftung		Unternehmen der Abfallbewirtschaftung im Sinne des Artikels 3 Nummer 9 der Richtlinie 2008/98/EG des Europäischen Parlaments und des Rates (1), ausgenommen Unternehmen, für die Abfallbewirtschaftung nicht ihre Hauptwirtschaftstätigkeit ist
3. Produktion, Herstellung und Handel mit chemischen Stoffen		Unternehmen im Sinne des Artikels 3 Nummern 9 und 14 der Verordnung (EG) Nr. 1907/2006 des Europäischen Parlaments und des Rates (2), 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
4. Produktion, Verarbeitung und Vertrieb von Lebensmitteln		Lebensmittelunternehmen im Sinne des Artikels 3 Nummer 2 der Verordnung (EG) Nr. 178/2002 des Europäischen Parlaments und des Rates (3), die im Großhandel sowie in der industriellen Produktion und Verarbeitung tätig sind
5. Verarbeitendes Gewerbe/Herstellung von Waren	a) Herstellung von Medizinprodukten und In-vitro-Diagnostika	Einrichtungen, die Medizinprodukte im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates (4) herstellen, und In-vitro- [illegible] des Artikels 2 Nummer [illegible]

- Achtung: nationale Umsetzung ebenfalls prüfen! Sektorspezifische Ausnahmen (Art. 4), wie DORA (Finanzmarkt) und für Luftfahrtunternehmen!

4. Anwendungsbereich – Welche Unternehmen („Einrichtungen“) fallen unter die Regulierung?

Achtung: vereinfachte Darstellung!

- Öffentliche und private Einrichtungen
- Sektoren
  - **Anhang I „Sektoren mit Hoher Kritikalität“:** Energie (Elektrizität, Fernwärme und –kälte, Erdöl, Erdgas, Wasserstoff), Verkehr (Luft-, Schienenverkehr, Schifffahrt, Strassenverkehr [Betreiber intelligenter Verkehrssysteme]), Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser, Abwasser, Digitale Infrastruktur, Verwaltung von IKT-Diensten (B2B), Öffentliche Verwaltung, Weltraum
  - **Anhang II „sonstige kritische Sektoren“:** Post- und Kurierdienste, Abfallbewirtschaftung, Produktion, Herstellung und Handel mit chemischen Stoffen, Produktion, Verarbeitung und Vertrieb von Lebensmitteln, Verarbeitendes Gewerbe/Herstellung von Waren (Medizinprodukte, Datenverarbeitungsgeräte, elektrische Ausrüstungen, Maschinenbau, Herstellung von Kraftwagen und Kraftwagenteilen, sonstiger Fahrzeugbau), Anbieter digitaler Dienste, Forschung
- Schwellenwert mittlere Unternehmen
  - weniger als 250 Mitarbeiter und ein Jahresumsatz von unter 50 Mio. EUR bzw. eine Jahresbilanz von unter 43 Mio. EUR
- Ausnahmen zu den Schwellenwerten (d.h. unabhängig von der Grösse der Einrichtungen)
  - Kommunikationsnetze, Vertrauensdiensteanbieter, Domänennamenregistrierer, kritische Einrichtungen nach Richtlinie (EU) 2022/2557 (i.e. KRITIS)

4. Anwendungsbereich: Begriffliche Klärung

- «***Einrichtungen***» im Geltungsbereich (Art. 2) => Sektoren und Schwellenwerte (ja/nein)

- 2 Kategorien (Art. 3): «***wesentliche Einrichtungen***» und «***wichtige Einrichtungen***» => Differenzierung bei Pflichten (Risikomanagementmassnahmen und Meldepflichten) und bei den Aufsichts- und Durchsetzungsregeln («wesentliche» => proaktiv; «wichtige» => reaktiv)
  - Wesentliche Einrichtungen sind insbesondere mittlere Unternehmen, qual. Vertrauensdiensteanbieter, Domänennamenregister und DNS-Diensteanbieter und «kritische Einrichtungen» gemäss Richtlinie (EU) 2022/25557 werden als wesentliche Einrichtungen eingestuft (Stichwort «KRITIS»)
  - Alle anderen Einrichtungen sind wichtige Einrichtungen.

➢ *Ob es sich um eine wesentliche oder eine wichtige Einrichtung handelt, hat begrifflich nichts mit der Frage zu tun, ob eine Einrichtung unter die NIS-2-Richtlinie fällt!*

4. Anwendungsbereich – Fallen auch CH-Unternehmen unter die NIS-2-Regulierung?

- Ja, wenn Einrichtungen Dienste („**vor Ort**“) erbringen oder tätig sind:

Artikel 2

Anwendungsbereich

(1) Diese Richtlinie gilt für öffentliche oder private Einrichtungen der in den Anhang I oder II genannten Art, die nach Artikel 2 des Anhangs der Empfehlung 2003/361/EG als mittlere Unternehmen gelten oder die Schwellenwerte für mittlere Unternehmen nach Absatz 1 jenes Artikels überschreiten und ihre Dienste in der Union erbringen oder ihre Tätigkeiten dort ausüben.

- Sonderregelung für bestimmte **grenzüberschreitende** Dienstleistungen (Domänennamensysteme (DNS); Cloud-Computing-Dienste (IaaS, PaaS, NaaS); Rechenzentrumsdienste (≠ interne Rechenzentren), etc.; siehe Art. 26
- Es geht nicht um Produkte (=> Cyber Resilience Act; neue EU-Produkthaftungsrichtline)!

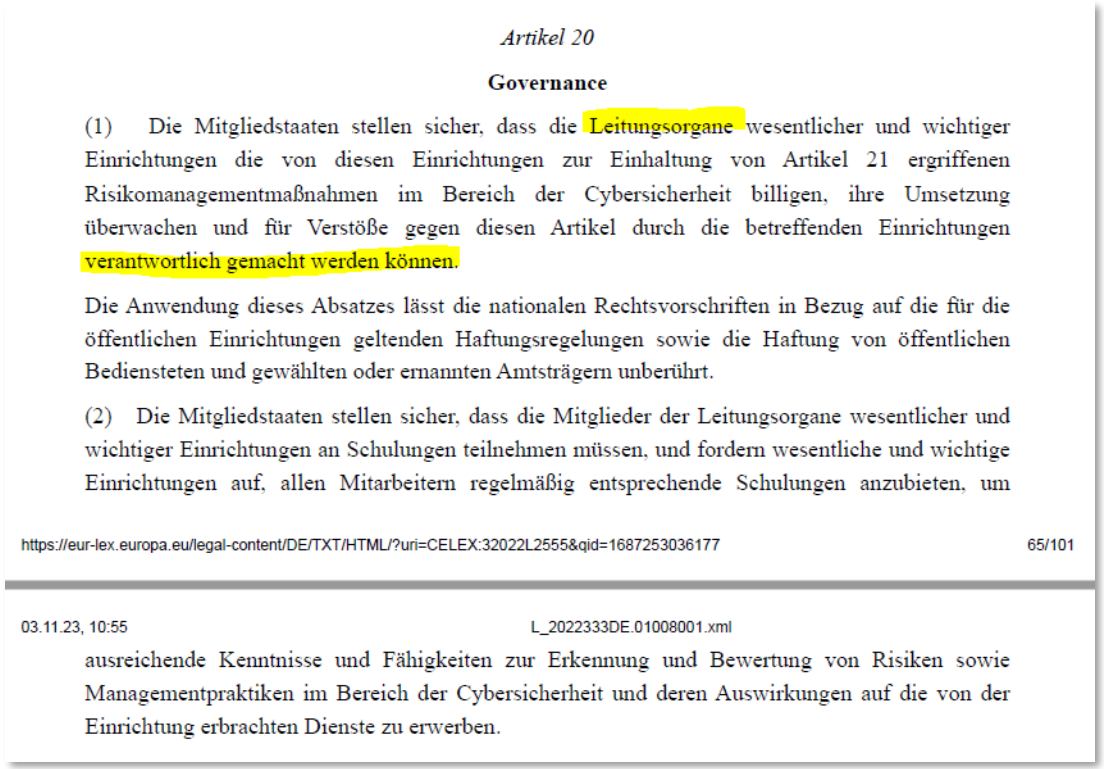
5. Übersicht über die Pflichten

- Governance (Art. 20)
- *Risikomanagementmassnahmen im Bereich Cybersicherheit (Art. 21)*
- *Koordinierte Risikobewertungen in Bezug auf die Sicherheit kritischer Lieferketten auf der Ebene der Union (Art. 22)*
- *Berichtspflichten (Art. 23)*
- Nutzung der europäischen Schemata für die Cybersicherheitszertifizierung (Art. 24)
- Vertreter in der Union (Art. 26 (3))
- Registrierung (Art. 27)

6. Governance

- Adressat: Wer?
  - Leitungsorgane wesentlicher und wichtiger Einrichtungen gem. Art. 3
- Pflicht: Was?
  - Risikomanagementmassnahmen (Billigung, Überwachung)
  - Verantwortlichkeit Leitungsorgane
  - Teilnahme an Schulungen
  - Schulung für alle Mitarbeiter

➢ Empfehlung: Dokumentation!



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

https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555&qid=1687253036177 65/101

03.11.23, 10:55 L_2022333DE.01008001.xml

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.

7. Vertreter in der Union – Art. 26 (3)

- Wer? Welche CH-Unternehmen?

  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 Sicherheits-diensten sowie Anbieter von Online-Marktplätzen, Online-Suchmaschinen oder Plattformen für Dienste sozialer Netzwerke

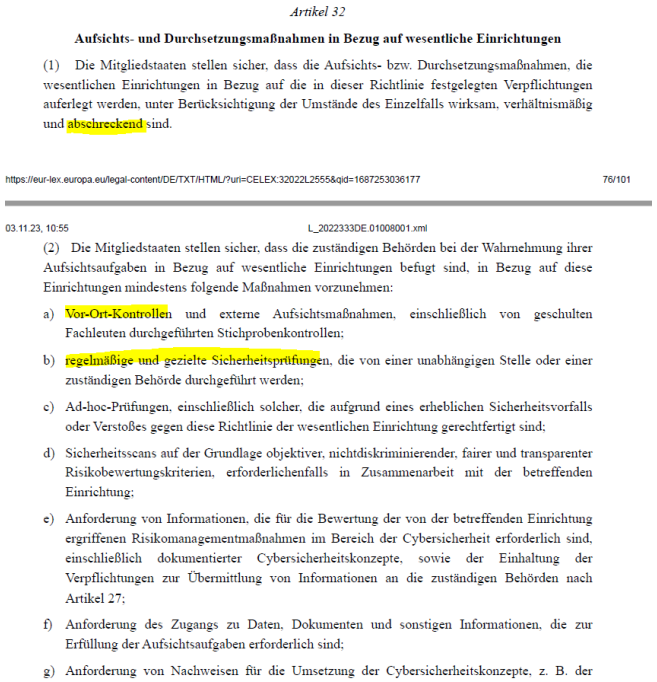
- Was? Meldung Vertreter (= Adresse)
- In welchem Land? Wahlrecht.
- Registrierung (Art. 27)
- Datenbank Domänennamen-Reg. Daten
- Achtung: Sanktionen!

(3) Hat eine in Absatz 1 Buchstabe b genannte Einrichtung keine Niederlassung in der Union, bietet aber Dienste innerhalb der Union an, muss sie einen Vertreter in der Union benennen. Der Vertreter muss in einem der Mitgliedstaaten niedergelassen sein, in denen die Dienste angeboten werden. Es wird davon ausgegangen, dass eine solche Einrichtung der Zuständigkeit des Mitgliedstaats unterliegt, in dem der Vertreter niedergelassen ist. Wurde in der Union kein Vertreter im Sinne dieses Absatzes benannt, kann jeder Mitgliedstaat, in dem die Einrichtung Dienste erbringt, gegen die Einrichtung rechtliche Schritte wegen des Verstoßes gegen diese Richtlinie einleiten.

(4) Die Benennung eines Vertreters durch eine in Absatz 1 Buchstabe b genannte Einrichtung lässt rechtliche Schritte, die gegen die Einrichtung selbst eingeleitet werden könnten, unberührt.

8. Aufsicht und Durchsetzung (31) – Wie setzt die EU die Pflichten durch?

- Aufsicht durch nationale Behörden (Art. 31)
- Massnahmen und Sanktionen (Art. 32, 33)
  - Aussetzung Zertifizierung
  - Untersagung Leitungsaufgaben
  - **Geldbussen** (Art. 34)
- Datenschutz (35)
- Sanktionen (36)
- Amtshilfe (37)
- Ausschussverfahren (38)
- ➢ **Fazit: Es gilt ernst!**
- ➢ Aber: Verfahrensgarantien



Artikel 32

Aufsichts- und Durchsetzungsmaßnahmen in Bezug auf wesentliche Einrichtungen

(1) Die Mitgliedstaaten stellen sicher, dass die Aufsichts- bzw. Durchsetzungsmaßnahmen, die wesentlichen Einrichtungen in Bezug auf die in dieser Richtlinie festgelegten Verpflichtungen auferlegt werden, unter Berücksichtigung der Umstände des Einzelfalls wirksam, verhältnismäßig und abschreckend sind.

https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555&qid=1687253036177 76/101

03.11.23, 10:55 L_2022333DE.01008001.xml

(2) Die Mitgliedstaaten stellen sicher, dass die zuständigen Behörden bei der Wahrnehmung ihrer Aufsichtsaufgaben in Bezug auf wesentliche Einrichtungen befugt sind, in Bezug auf diese Einrichtungen mindestens folgende Maßnahmen vorzunehmen:

a) Vor-Ort-Kontrollen und externe Aufsichtsmaßnahmen, einschließlich von geschulten Fachleuten durchgeführten Stichprobenkontrollen;

b) regelmäßige und gezielte Sicherheitsprüfungen, die von einer unabhängigen Stelle oder einer zuständigen Behörde durchgeführt werden;

c) Ad-hoc-Prüfungen, einschließlich solcher, die aufgrund eines erheblichen Sicherheitsvorfalls oder Verstoßes gegen diese Richtlinie der wesentlichen Einrichtung gerechtfertigt sind;

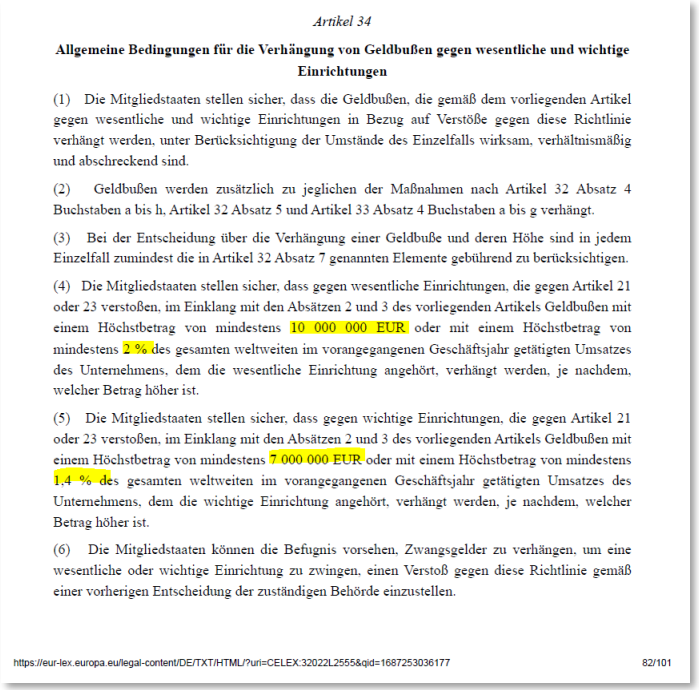
d) Sicherheitsscans auf der Grundlage objektiver, nichtdiskriminierender, fairer und transparenter Risikobewertungskriterien, erforderlichenfalls in Zusammenarbeit mit der betreffenden Einrichtung;

e) Anforderung von Informationen, die für die Bewertung der von der betreffenden Einrichtung ergriffenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit erforderlich sind, einschließlich dokumentierter Cybersicherheitskonzepte, sowie der Einhaltung der Verpflichtungen zur Übermittlung von Informationen an die zuständigen Behörden nach Artikel 27;

f) Anforderung des Zugangs zu Daten, Dokumenten und sonstigen Informationen, die zur Erfüllung der Aufsichtsaufgaben erforderlich sind;

g) Anforderung von Nachweisen für die Umsetzung der Cybersicherheitskonzepte, z. B. der Ergebnisse von Sicherheitsprüfungen, die von einem qualifizierten Prüfer durchgeführt wurden, und der entsprechenden zugrunde liegenden Nachweise.

Die in Unterabsatz 1 Buchstabe b genannten gezielten Sicherheitsprüfungen stützen sich auf Risikobewertungen, die von der zuständigen Behörde oder der geprüften Einrichtung durchgeführt werden, oder auf sonstige verfügbare risikobezogene Informationen.



Artikel 34

Allgemeine Bedingungen für die Verhängung von Geldbußen gegen wesentliche und wichtige Einrichtungen

(1) Die Mitgliedstaaten stellen sicher, dass die Geldbußen, die gemäß dem vorliegenden Artikel gegen wesentliche und wichtige Einrichtungen in Bezug auf Verstöße gegen diese Richtlinie verhängt werden, unter Berücksichtigung der Umstände des Einzelfalls wirksam, verhältnismäßig und abschreckend sind.

(2) Geldbußen werden zusätzlich zu jeglichen der Maßnahmen nach Artikel 32 Absatz 4 Buchstaben a bis h, Artikel 32 Absatz 5 und Artikel 33 Absatz 4 Buchstaben a bis g verhängt.

(3) Bei der Entscheidung über die Verhängung einer Geldbuße und deren Höhe sind in jedem Einzelfall zumindest die in Artikel 32 Absatz 7 genannten Elemente gebührend zu berücksichtigen.

(4) Die Mitgliedstaaten stellen sicher, dass gegen wesentliche Einrichtungen, die gegen Artikel 21 oder 23 verstoßen, im Einklang mit den Absätzen 2 und 3 des vorliegenden Artikels Geldbußen mit einem Höchstbetrag von mindestens 10 000 000 EUR oder mit einem Höchstbetrag von mindestens 2 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens, dem die wesentliche Einrichtung angehört, verhängt werden, je nachdem, welcher Betrag höher ist.

(5) Die Mitgliedstaaten stellen sicher, dass gegen wichtige Einrichtungen, die gegen Artikel 21 oder 23 verstoßen, im Einklang mit den Absätzen 2 und 3 des vorliegenden Artikels Geldbußen mit einem Höchstbetrag von mindestens 7 000 000 EUR oder mit einem Höchstbetrag von mindestens 1,4 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens, dem die wichtige Einrichtung angehört, verhängt werden, je nachdem, welcher Betrag höher ist.

(6) Die Mitgliedstaaten können die Befugnis vorsehen, Zwangsgelder zu verhängen, um eine wesentliche oder wichtige Einrichtung zu zwingen, einen Verstoß gegen diese Richtlinie gemäß einer vorherigen Entscheidung der zuständigen Behörde einzustellen.

https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555&qid=1687253036177 82/101

9. Empfehlungen aus juristischer Sicht – Roadmap

- Schritt 1:
  - ➢ Abklärung der Anwendbarkeit. Falle ich unter die Regulierung? Dokumentierung (Schutz GL/VR)!
- Schritt 2:
  - ➢ Gap-Analyse – Pflichten vs. vorhandene TOM
- Schritt 3:
  - ➢ Massnahmenplan
- Schritt 4:
  - ➢ Governance, Prozessdokumentation, jur. Kontrolle Umsetzung
- Schritt 5:
  - ➢ Meldung Vertreter notwendig?

➢ Budget

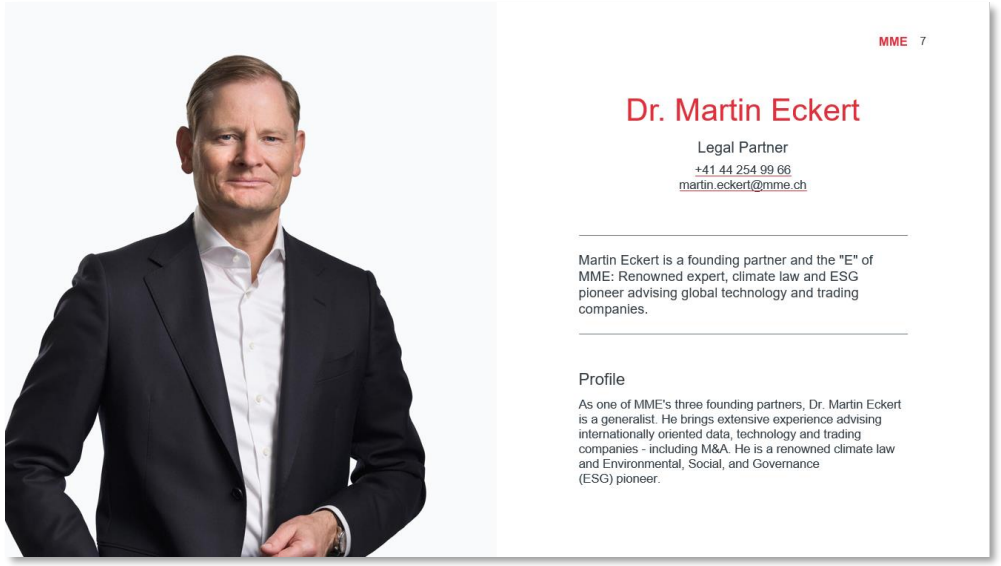
E.2 Erfüllungsaufwand für die Wirtschaft

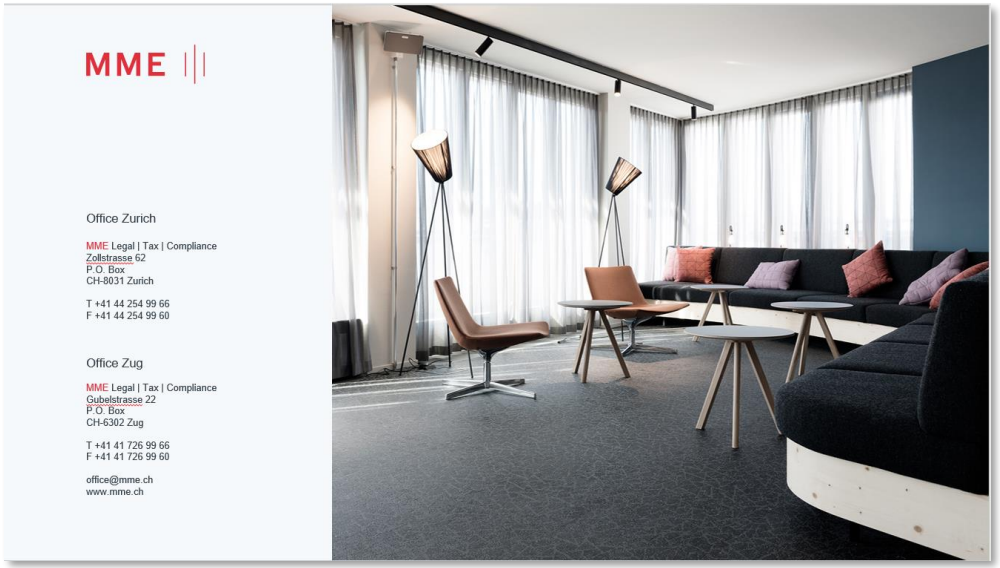
Für die Wirtschaft erhöht sich der jährliche Erfüllungsaufwand um rund 2,3 Milliarden Euro. Insgesamt entsteht einmaliger Aufwand von rund zwei Milliarden Euro. Dieser ist fast ausschließlich der Kategorie Einführung oder Anpassung digitaler Prozessabläufe zuzuordnen.

Davon Bürokratiekosten aus Informationspflichten

Es entfallen rund 121 Millionen Euro auf Bürokratiekosten aus Informationspflichten.

SNV
standards connect
the world





Martin Eckert, MME Legal Tax Compliance, Legal Partner

Zürich, 03. Juli 2024

Schweizerische Normen-Vereinigung (SNV)
Association Suisse de Normalisation (SNV)
Swiss Association for Standardization (SNV)

Sulzerallee 70, Postfach
CH-8404 Winterthur/Switzerland, T +41 52 224 54 54
info@snv.ch, www.snv.ch

Member
International Organization for Standardization (ISO)
Comité Européen de Normalisation (CEN)

SNV
standards connect
the world

Danke für Ihre Aufmerksamkeit