

# NIS II

## Sind auch Sie betroffen?!

e-Government und e-Health Konferenz 2022

Mag. Vinzenz Heußler, LL.M.

Bundeskanzleramt, Abteilung I/8 (Cyber Security, GovCERT, NIS-Büro und ZAS)

Leiter NIS-Büro

Salzburg, 6. September 2022

## Die neue NIS-Richtlinie (NIS2)

- **NIS 2**: Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148
  - Von EU-Kommission (DG CONNECT) am 16.12.2020 als Teil der neuen EU-Cybersicherheitsstrategie vorgelegt
- NIS 2 ersetzt **NIS 1** = Richtlinie (EU) 2016/1148 vom 6. Juli 2016
  - 1. Rechtsakt über Cybersicherheit in EU
  - Legt Maßnahmen fest, mit denen ein hohes gemeinsames Sicherheitsniveau von Netz- und Informationssystemen in der EU erreicht werden soll

## NIS 1 – „Probleme“

- Unzureichendes Niveau der **Cyber-Resilienz** von Unternehmen aufgrund von
  - fehlenden Cybersicherheitsmaßnahmen (aufgrund der Nichtberücksichtigung)
  - uneinheitlicher Behandlung im gesamten Binnenmarkt (Diskrepanzen in den Ermittlungen der Betreiber)
- **Unterschiedlich starke** Resilienz der Mitgliedstaaten und Sektoren
- Schwach ausgeprägte **gemeinsame Lageerfassung** und mangelnde gemeinsame **Krisenreaktion**

## Was will NIS 2 besser machen?

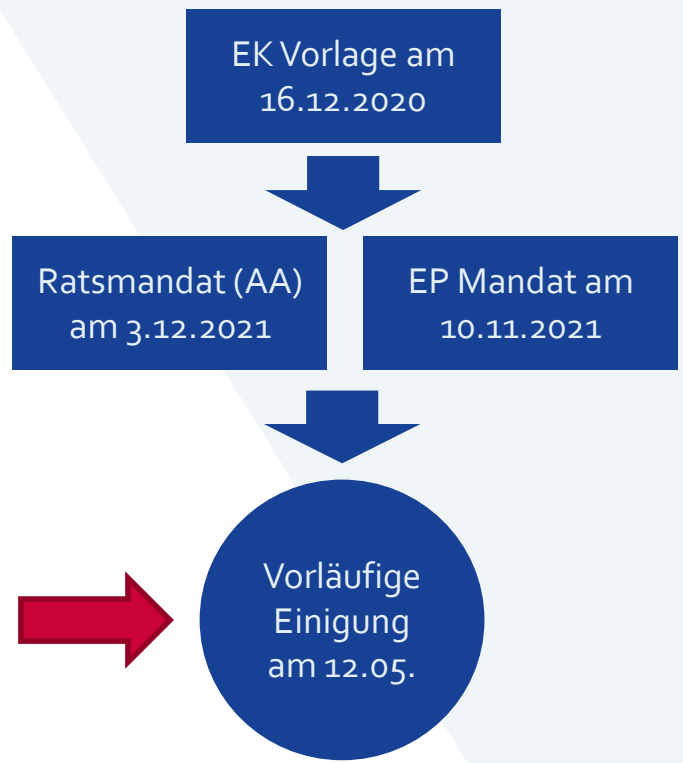
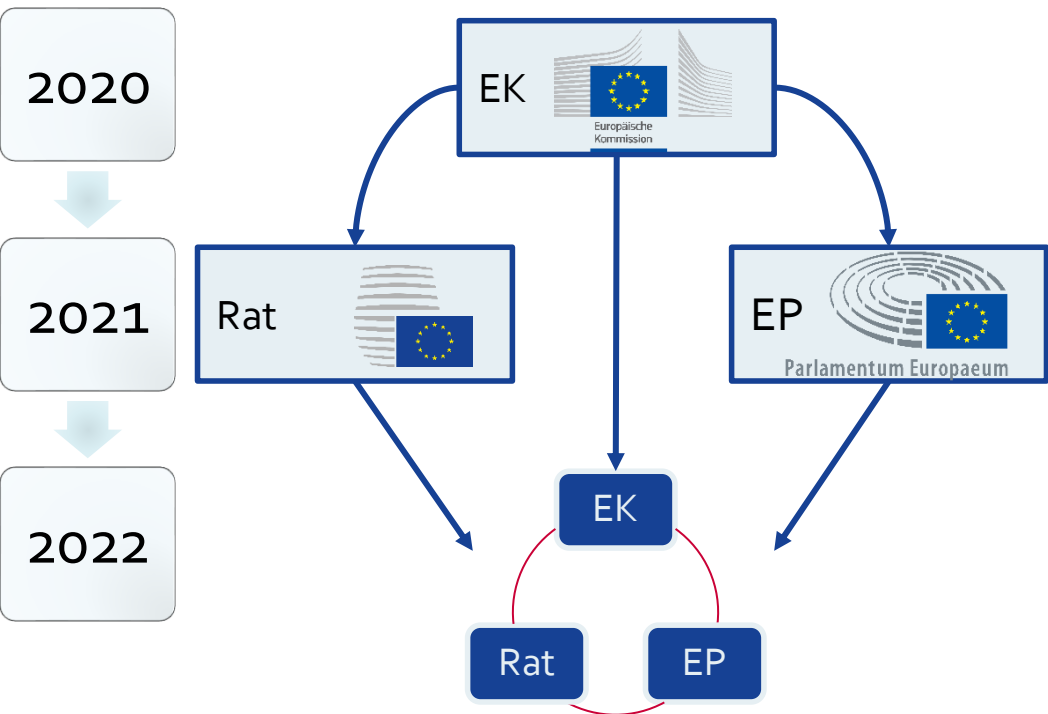
- 1. Stärkung der Cyberresilienz eines alle relevanten Sektoren umfassenden Spektrums von Unternehmen,**
  - alle öffentlichen und privaten Einrichtungen im gesamten Binnenmarkt, die wichtige Funktionen für die Wirtschaft und die Gesellschaft als Ganzes erfüllen, sollen verpflichtet werden, angemessene Cybersicherheitsmaßnahmen zu ergreifen
  
- 2. Förderung einer gleich starken Resilienz bei den bereits unter die Richtlinie fallenden Sektoren im Binnenmarkt, durch weitere Angleichung**
  1. des De-facto-Anwendungsbereichs,
  2. der Sicherheitsanforderungen und Meldepflichten bei Sicherheitsvorfällen,
  3. der Bestimmungen für die nationale Aufsicht und Durchsetzung sowie
  4. der Kapazitäten der zuständigen Behörden in den Mitgliedstaaten.

## Was will NIS 2 besser machen?

### 3. Verbesserung der gemeinsamen Lageerfassung und der kollektiven Vorsorge und Reaktionsfähigkeit

- Maßnahmen zur Stärkung des Vertrauens zwischen den zuständigen Behörden
- verstärkten des Informationsaustauschs
- Festlegung von Regeln und Verfahren im Falle weitreichender Sicherheitsvorfälle oder Krisen

# Trilogie



## Zeitplan auf EU-Ebene

Vorläufige politische Einigung im 3. Trilog	12. Mai
Finalisierung des Textes auf technischer Ebene	Ende Mai - Mitte Juni
Konsolidierter Text von AStV I gebilligt	22. Juli
Bericht des Berichterstatters von ITRE-Ausschuss gebilligt	13. Juli
<b>Sprachjuristische Prüfung und Finalisierung der EN Sprachfassung</b>	<b>August - Mitte Sept</b>
Übersetzung in 23 Amtssprachen und Prüfung	September
Annahme durch Plenum des EP (1. Lesung)	Oktober
Finale Annahme durch Rat	Ende Oktober

## Zeitplan auf EU-Ebene

Signatur, Übermittlung an Büro des ABI der EU & Veröffentlichung im ABI	November
Inkrafttreten 20 Tage nach Veröffentlichung im ABI	Ende November
21 Monate Umsetzungsfrist für Mitgliedstaaten	August 2024



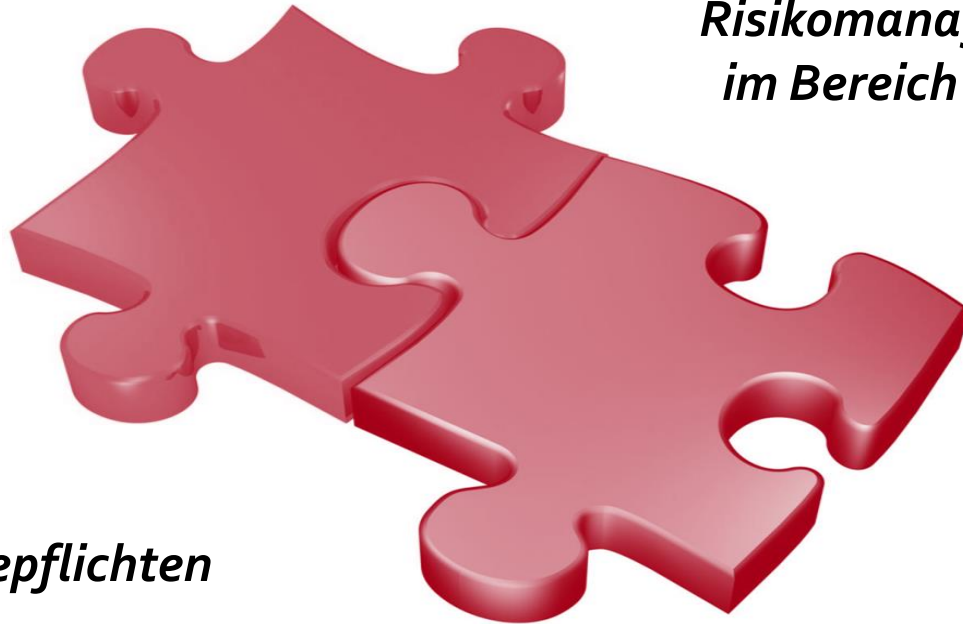
# Die drei Säulen von NIS2

Mitgliedstaaten	Kooperation und Informationsaustausch	Risikomanagement
Nationale Behörden	NIS-Kooperationsgruppe Peer-Review	Verantwortlichkeit des Top-Managements
CSIRTs	CSIRTs-Netzwerk	Trainings für Top-Managements
Krisenmanagement	CyCLONE	Unterscheidung wesentliche und wichtige Einrichtungen
Nationale Strategien	ENISA Cybersecurity Reports	Einrichtungen sind verpflichtet, Sicherheitsmaßnahmen zu ergreifen
Rahmen für CVD (Coordinated Vulnerability Disclosure)	Europäisches Schwachstellenregister	Einrichtungen sind verpflichtet, signifikante Vorfälle zu melden

Rot = Neuerungen gegenüber NIS1

## NIS 2 – Verpflichtungen für Einrichtungen

*Risikomanagementmaßnahmen  
im Bereich der Cybersicherheit*



*Meldepflichten*

## Sicherheitsanforderungen

- Verantwortung des **Top-Managements** bei Nichteinhaltung von Maßnahmen des CS Risikomanagements
- **Schulungen für Top-Management**
- **Risikobasierter Ansatz:** angemessene und verhältnismäßige technische und organisatorische Maßnahmen
- **All-Gefahren-Ansatz** (All-hazards approach) mit dem Ziel, Netz- und Informationssysteme sowie ihre physische Umgebung vor Störungen zu schützen

# Sicherheitsanforderungen

- a) Risikoanalyse und Sicherheitsrichtlinien für Informationssysteme
- b) Behandlung von Vorfällen
- c) Business Continuity (inkl. Backup-Management und Notfallwiederherstellung) und Krisenmanagement
- d) Supply Chain Security (inkl. sicherheitsbezogene Aspekte der Beziehungen mit direkten Anbietern oder Diensteanbietern)
- e) Sicherheit bei der Beschaffung, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Umgang mit Schwachstellen und deren Offenlegung

## Sicherheitsanforderungen

- f) Richtlinien und Verfahren zur Bewertung der Wirksamkeit von Cyber-Risikomanagementmaßnahmen
- g) Grundlegende Praktiken der Cyberhygiene und Schulungen zur Cybersicherheit
- h) Richtlinien und Verfahren zum Einsatz von Kryptografie und, wo angemessen, Verschlüsselung
- i) Sicherheit der Humanressourcen, Zugangskontrollmaßnahmen und Vermögensverwaltung
- j) Verwendung von Lösungen für die MFA oder die kontinuierliche Authentifizierung, die gesicherte Sprach-, Video- und Textkommunikation sowie ggf gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung

# Meldepflichten

## Stärker harmonisierte Meldepflichten

- Einrichtungen müssen signifikante Cybersicherheits-Vorfälle melden
- Einrichtungen müssen Dienst-Empfänger über signifikante Cybersicherheits-Vorfälle und –Bedrohungen informieren, wenn angemessen
- Meldeprozess:

Early Warning 24h  
Erstmeldung 72h

Zwischenbericht  
auf Anfrage der CA  
oder des CSIRT

Abschlussbericht  
innerhalb eines  
Monats

## Meldepflichten

- Ein Sicherheitsvorfall gilt als signifikant, wenn
  - a) er erhebliche Betriebsstörungen oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann;
  - b) er andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Verluste geschädigt hat oder schädigen kann.
- EU-Kommission kann (und muss im Sektor digitale Infrastruktur) in Durchführungsrechtsakten festlegen, wann ein Vorfall signifikant ist.

## Aufsicht

- Mindestliste an **Aufsichtsmaßnahmen** (regelmäßige & gezielte Audits, Vor-Ort- & Off-Site-Kontrollen, Sicherheitsscans) und **Mittel**, die den **zuständigen Behörden** zur Verfügung stehen (Ersuchen um Informationen & Zugang zu Beweismitteln).
- **Differenzierung des Aufsichtssystems** zwischen wesentlichen und wichtigen Unternehmen, um ein faires Gleichgewicht zwischen den Verpflichtungen der Einrichtungen und der zuständigen Behörden zu gewährleisten:
  - vollwertige Aufsicht (**ex ante & ex post**) für wesentliche Einrichtungen und
  - **ex post** Aufsicht für wichtige Einrichtungen.
- Risikobasierte Aufsicht möglich



## Durchsetzung

- Mindestliste von **Verwaltungssanktionen** (z. B. verbindliche Anweisungen, Verwaltungsstrafen)
- Maximale **Bußgeldhöhe**:
  - mind. 10.000.000 EUR oder 2% des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres für wesentliche Einrichtungen
  - mind. 7.000.000 EUR oder 1,4% für wichtige Einrichtungen
- Natürliche Personen (leitende Angestellte) können für Pflichtverletzungen haftbar gemacht werden

# Anwendungsbereich: Wesentliche und wichtige Einrichtungen

Wesentliche Einrichtungen	Wichtige Einrichtungen
Energie (Elektrizität*, Fernwärme/Kälte, Öl, Gas und Wasserstoff)	Post- und Kurierdienste
Verkehr (Luft, Schiene, Schifffahrt, Straße)	Abfallbewirtschaftung
Bankwesen	Chemie (Herstellung und Handel)
Finanzmarktinfrastrukturen	Lebensmittel (Produktion, Verarbeitung, Vertrieb)
Gesundheitswesen (Gesundheitsdienstleister, EU-Referenzlaboratorien, Forschung und Herstellung von pharmazeutischen und medizinischen Produkten und Geräte)	Verarbeitendes / Herstellendes Gewerbe (Medizinprodukten; Datenverarbeitungs-, elektronische und optische Geräte und elektronische Ausrüstungen; Maschinenbau; Kraftwagen und Kraftwagenteile und sonstiger Fahrzeugbau)
Trinkwasser	Anbieter digitaler Dienste (Suchmaschinen, online-Marktplätze und Plattformen für Dienste sozialer Netzwerke)
Abwasser	
Digitale Infrastruktur (IXP, DNS, TLD, Cloud-Computing, Rechenzentren, Inhaltzustellnetzen (CDN), Vertrauensdiensteanbieter und öffentliche elektronische Kommunikationsnetze)	
Öffentliche Verwaltung	
Weltraum	

Rot = Neuerungen gegenüber NIS1

Energie (Elektrizität, **Betreiber einer Ladestation**, Fernwärme/Kälte, Öl, Gas und Wasserstoff)

Post- und Kurierdienste

Verkehr (Luft [**kommerziell**], Schiene, Schifffahrt, Straße [**ohne Straßenbehörden, wenn nur Nebenaktivität**])

Abfallbewirtschaftung

Bankwesen

Chemie (Herstellung und Handel + **Hersteller von Artikeln gem Art 3(3) VO (EG) Nr 1907/2006**)

Finanzmarktinfrastrukturen

Lebensmittel (Produktion, Verarbeitung, Vertrieb, **wenn Großhandel und industrielle Produktion und Verarbeitung**)

Gesundheitswesen

(Gesundheitsdienstleister, EU-Referenzlaboratorien, Forschung und Herstellung von pharmazeutischen und medizinischen Produkten und Geräte)

Verarbeitendes / Herstellendes Gewerbe

(Medizinprodukten; Datenverarbeitungs-, elektronische und optische Geräte und elektronische Ausrüstungen; Maschinenbau; Kraftwagen und Kraftwagenteile und sonstiger Fahrzeugbau)

Trinkwasser

Anbieter digitaler Dienste (Suchmaschinen, Online-Marktplätze und Plattformen für Dienste sozialer Netzwerke)

Abwasser (**Ausnahme, wenn nur Nebenaktivität**)

**Forschung (Forschungseinrichtungen)**

Digitale Infrastruktur

(IXP, DNS [**außer Betreiber von Root Name Server**], TLD, Cloud, Rechenzentren, Inhaltzustellnetzen (CDN), VDA und ECS & ECN)

**Lila = Änderungen durch Verhandlungen**

**IKT – Service Management**

(**Managed service providers und Managed Security service providers**)

Öffentliche Verwaltung (**Zentralregierungen + regionale Ebene**)

Weltraum

## Anwendungsbereich

- NIS1: Mitgliedstaaten hatten großen Ermessensspielraum bei der Ermittlung der Betreiber wesentlicher Dienste.
- NIS2: Anwendungsbereich durch „**size cap rule**“ grds vorgegeben.
  - NIS2 gilt für alle öffentliche oder private wesentliche und wichtige Einrichtungen der in Anhang I und Anhang II genannten Art, die ihre Dienstleistungen in der EU erbringen oder ihre Tätigkeiten in der EU ausüben und die den Schwellenwert für mittlere Unternehmen iSd Empfehlung 2003/361/EG der EU-Kommission erreichen oder überschreiten


## Anwendungsbereich

- Prüfschema („Bin ich betroffen?“ „Bin ich wesentlich oder wichtig?“):
  - Erbringt die Einrichtung ihre Dienstleistungen in der EU oder übt ihre Tätigkeiten in der EU aus? („Serviciere ich den Binnenmarkt“?)
  - Entspricht die Einrichtung einer in Spalte 3 von Anhang I und Anhang II genannten Art? („Führt mich die NIS2 an?“ „In welchem Anhang“?)
  - Erreicht oder überschreitet die Einrichtung den Schwellenwert für mittlere Unternehmen? („Wie groß bin ich?“)
- Achtung: Es gibt Ausnahmen und Sonderregeln!

## Entspricht die Einrichtung einer in Spalte 3 von Anhang I und Anhang II genannten Art?


Sektor	Teilsektor	Art der Einrichtung
1.Energie	a) Elektrizität	Verteilernetzbetreiber im Sinne des Artikels 2 Nummer 29 der Richtlinie (EU) 2019/944

3. Spalte Anhang I



Art der Einrichtung	Nationale Begriffsbestimmungen
Verteilernetzbetreiber im Sinne des § 7 Abs 1 Z. 76 EIWOG	Verteilernetzbetreiber (§ 7 Abs 1 Z. 76 EIWOG) = eine natürliche oder juristische Person oder eingetragene Personengesellschaft, die verantwortlich ist für den Betrieb, die Wartung sowie erforderlichenfalls den Ausbau des Verteilernetzes in einem bestimmten Gebiet und gegebenenfalls der Verbindungsleitungen zu anderen Netzen sowie für die Sicherstellung der langfristigen Fähigkeit des Netzes, eine angemessene Nachfrage nach Verteilung von Elektrizität zu befriedigen.

Referenz im nationalen Recht



## Schwellenwerte

- Kleinstunternehmen: ein Unternehmen, das weniger als **10 Personen** beschäftigt **und** dessen Jahresumsatz bzw. Jahresbilanz **2 Mio. EUR** nicht überschreitet.
- Kleines Unternehmen: ein Unternehmen, das weniger als **50 Personen** beschäftigt **und** dessen Jahresumsatz bzw. Jahresbilanz **10 Mio. EUR** nicht übersteigt.
- Mittleres Unternehmen: ein Unternehmen, das weniger als **250 Personen** beschäftigen **und** die entweder einen Jahresumsatz von höchstens **50 Mio. EUR** erzielen **oder** deren Jahresbilanzsumme sich auf höchstens **43 Mio. EUR** beläuft.
- Großunternehmen: Alle Unternehmen, sofern kein KMU.

## Wann fallen Kleinunternehmen unter die NIS2?

- Bestimmte Arten von Einrichtungen im Sektor Digitale Infrastruktur.
- Nach CER-Richtlinie als kritische Einrichtung ermittelt.
- Staat stuft Kleinunternehmen als wichtig oder wesentlich ein. Kriterien:
  - Einziger Erbringer eines Dienstes, der für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Tätigkeiten wesentlich ist.
  - Unterbrechung der Dienstleistung könnte erhebliche Auswirkungen auf die öffentliche Sicherheit, die öffentliche Ordnung oder die öffentliche Gesundheit haben.
  - Unterbrechung der Dienstleistung könnte ein erhebliches Systemrisiko mit sich bringen (insb. grenzüberschreitende Auswirkungen).
  - Besondere Bedeutung auf regionaler oder nationaler Ebene für den betreffenden Sektor oder die betreffende Art von Dienstleistung oder für andere voneinander abhängige Sektoren kritisch.



## Wesentliche und wichtige Einrichtungen

- Wesentliche Einrichtungen
  - Alle im Anhang I angeführten Einrichtungen, welche die Schwellenwerte für mittlere Unternehmen überschreiten.
- Wichtige Einrichtungen
  - Alle anderen Einrichtungen.
- Ausnahmen:
  - Sektoren Digitale Infrastruktur und Öffentliche Verwaltung
  - Immer wesentlich: Nach CER-Richtlinie als kritische Einrichtung ermittelt.

# Grundregel Anwendungsbereich Anhang I

Sektoren	Groß- unter- nehmen	Mittlere Unter- nehmen	Kleinst- und Klein- unternehmen
Anhang I			
Energie / Verkehr / Bankwesen / Finanzmarktinfrastrukturen / <b>Gesundheitswesen</b> / Trinkwasser / Abwasser / IKT-Service Management / Weltraum			

- Großunternehmen: wesentlich.
- Mittlere Unternehmen: Wichtig, außer falls ermittelt als wesentlich.
- Kleinst- und Kleinunternehmen: Nicht im Anwendungsbereich, außer falls ermittelt als wesentlich oder wichtig

## Sektor Gesundheitswesen (Grundregel)

- Gesundheitsdienstleister iSd Art 3 lit g der RL 2011/24/EU
- EU-Referenzlaboratorien iSd Art 15 der VO XXXX/XXXX zu schwerwiegenden grenzüberschreitenden Gesundheitsgefahren
- Einrichtungen, die Forschungs- und Entwicklungstätigkeiten in Bezug auf Arzneimittel iSd Art 1 Nr 2 der RL 2001/83/EG
- Einrichtungen, die pharmazeutische Erzeugnisse iSd Abschnitts C Abteilung 21 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) herstellen
- Einrichtungen, die Medizinprodukte herstellen, die während einer Notlage im Bereich der öffentlichen Gesundheit als kritisch iSd Art 20 der VO XXXX22 („Liste kritischer Medizinprodukte für Notlagen im Bereich der öffentlichen Gesundheit“) eingestuft werden.

## Sektor Digitale Infrastruktur (Sonderregeln)

Sektor	Art der Einrichtung	Große Unternehmen	Mittlere Unternehmen	Kleinst- und Kleinunternehmen
Anhang I				
Digitale Infrastruktur	TLD-Namenregister	Wesentlich		
	DNS-Diensteanbieter (ausgenommen Betreiber von Root-Nameserver)			
	Qualifizierte Vertrauensdiensteanbieter			
	Anbieter öffentlicher elektronischer Kommunikationsnetze oder Anbieter elektronischer Kommunikationsdienste, soweit deren Dienste öffentlich zugänglich sind	Wesentlich		Wichtig, außer falls ermittelt als <b>wesentlich</b>
	Vertrauensdiensteanbieter	Wesentlich	Wichtig, außer falls ermittelt als <b>wesentlich</b>	Nicht im Anwendungsbereich, außer falls ermittelt als <b>wesentlich</b> oder <b>wichtig</b>
	Betreiber von Internet-Knoten			
	Anbieter von Cloud-Computing-Diensten			
	Anbieter von Rechenzentrumsdiensten			
Betreiber von Inhaltzustellnetzen				

## Grundregel Anwendungsbereich Anhang II

Sektoren	Groß- unter- nehmen	Mittlere Unter- nehmen	Kleinst- und Klein- unternehmen
Anhang II			
Post- und Kurierdienste / Abfallbewirtschaftung / Lebensmittel / Verarbeitendes Gewerbes bzw. Herstellung von Waren / Anbieter digitaler Dienste / Forschung			

- Großunternehmen: Wichtig, außer falls ermittelt als wesentlich.
- Mittlere Unternehmen: Wichtig, außer falls ermittelt als wesentlich.
- Kleinst- und Kleinunternehmen: Nicht im Anwendungsbereich, außer falls ermittelt als wesentlich oder wichtig

## Sektor Öffentliche Verwaltung

- Bundes- und Landesebene grundsätzlich im Anwendungsbereich.
- Definition: „Einrichtung der öffentlichen Verwaltung“ ist eine Einrichtung, die
  1. zum Zweck gegründet wurde, im **allgemeinen Interesse** liegende Aufgaben zu erfüllen (hat keinen gewerblichen oder kommerziellen Charakter);
  2. **Rechtspersönlichkeit** besitzt oder gesetzlich befugt ist, im Namen einer anderen Einrichtung mit Rechtspersönlichkeit zu handeln;

## Sektor Öffentliche Verwaltung

- Definition: „Einrichtung der öffentlichen Verwaltung“ ist eine Einrichtung, die
  3. überwiegend vom Staat, einer Gebietskörperschaft oder von anderen Körperschaften des öffentlichen Rechts **finanziert** wird, oder deren Leitung der **Aufsicht** dieser Körperschaften untersteht, oder die über ein **Verwaltungs-, Leitungs- bzw. Aufsichtsorgan**, das mehrheitlich aus Mitgliedern besteht, die vom Staat, von Gebietskörperschaften oder von anderen Körperschaften des öffentlichen Rechts eingesetzt worden sind, verfügt;
  4. befugt ist, an natürliche oder juristische Personen **Verwaltungs- oder Regulierungsentscheidungen** zu richten, die deren Rechte im **grenzüberschreitenden Personen-, Waren-, Dienstleistungs- oder Kapitalverkehr** berühren.

## Sektor Öffentliche Verwaltung

- Im Anwendungsbereich sind
  - Einrichtungen der öffentlichen Verwaltung der **Zentralregierungen**, wie sie vom Staat nach nationalem Recht definiert werden.
  - Einrichtungen der öffentlichen Verwaltung auf **regionaler Ebene**, wie
    1. sie vom Staat im Einklang mit dem nationalen Recht festgelegt wurden und
    2. die nach einer risikobasierten Bewertung Dienstleistungen erbringen, deren Unterbrechung erhebliche Auswirkungen auf kritische gesellschaftliche oder wirtschaftliche Aktivitäten haben könnte.



## Sektor Öffentliche Verwaltung

- Ausgenommen:
  - Justiz, der Parlamente und der Zentralbanken
  - Bereiche nationale Sicherheit, Verteidigung, öffentliche Sicherheit oder Strafverfolgung

# Danke für Ihre Aufmerksamkeit!

Mag. Vinzenz Heußler, LL.M.

Bundeskanzleramt, Abteilung I/8 (Cyber Security, GovCERT, NIS-Büro und ZAS)

Leiter NIS-Büro

Wien, 6. September 2022