aringer herbst winklbauer

Bundeskanzleramt

NIS 2 RICHTLINIE –
es besteht dringender Handlungsbedarf

15. Oktober 2023
CIO Kongress , Loipersdorf

Dr. Stephan Winklbauer, LL.M.
Partner, Rechtsanwalt

Ing. Clemens Möslinger, BA MSc
Bundeskanzleramt, Abteilung I/8 (Technologie- und Datenmanagement, Cybersicherheit und Krisenrechenzentrum)

AGENDA

- **NIS 2** – was ist das?
  - **Warum** ist NIS 2 jetzt **interessant** für mich?
  - **Wen** betrifft das und was ist neu? (Anwendungsbereich)
  - **Was** ist jetzt zu tun? (Risikomanagementmaßnahmen)
  - **Prüfschema**
  - **Besonderheiten** von NIS 2 – Parallelen und Unterschiede zur DSGVO
- **Berichtspflichten**
- **Aufsicht** und **Durchsetzung**
- **Diskussion** und **Wrap-up**
  - Die **3 Säulen** von NIS 2
  - **Hauptziele**
  - **Herausforderungen** und **Take-Aways**

NIS 2 – DIE NEUE CYBERSICHERHEITSRICHTLINIE

- **N**etz- und **I**nformationssystem**S**icherheit
- **Richtlinie** vom 14. Dezember 2022 über Maßnahmen für ein **hohes gemeinsames Cybersicherheitsniveau** in der Union
- EU-weite horizontale Gesetzgebung
- **Modernisierung** des Rechtsrahmens:
  - Zunehmende Digitalisierung
  - Entwicklung der Bedrohungslandschaft
  - Defizite von NIS1
- Bis **17. Oktober 2024** in nationales Recht umzusetzen (→ NIS-Gesetz und NIS-Verordnungen)

WARUM IST NIS 2 JETZT INTERESSANT FÜR MICH?

Schärfere Sanktionsregeln – direkte Haftung der Unternehmensleitung mit eigenem Privatvermögen; vorübergehende behördliche Untersagung der Geschäftsführung

Umfangreichere Maßnahmen – Umsetzung bedarf massiver organisatorischer Eingriffe

Vorbereitung – Umsetzung bis zum Inkrafttreten des nationalen Umsetzungsgesetzes in der Verantwortung der Unternehmensleitung

WEN BETRIFFT NIS 2?

- **Size cap rule –** Anwendungsbereich abhängig von Unternehmensgröße
  - **Große** und **Mittlere** Unternehmen
  - In bestimmten Fällen Anwendung **unabhängig** von Unternehmensgröße (**Digitale Infrastruktur**)
  - **Öffentliche** und **private** Einrichtungen
  - Wesentliches Kriterium – **Art der Einrichtung** (Anhang I & II)

PRÜFSCHEMA

1. Erbringt das Unternehmen seine **Dienstleistungen in der EU** oder übt seine Tätigkeit in der EU aus?

2. Entspricht das Unternehmen einer in **Spalte 3 von Anhang I oder II** genannten Art?

3. Wie **groß** ist das Unternehmen? (Ausnahmen und Sonderregeln berücksichtigen!)

4. Ist das Unternehmen eine **wesentliche oder wichtige Einrichtung**?

UNTERNEHMEN AUS SPALTE 3 ANHANG I ODER ANHANG II?

Sektor	Teilsektor	Art der Einrichtung
1. Energie	a) Elektrizität	— Elektrizitätsunternehmen im Sinne des Artikels 2 Nummer 57 der Richtlinie (EU) 2019/944[1], die die Funktion „Versorgung“ im Sinne des Artikels 2 Nummer 12 jener Richtlinie wahrnehmen
		— Verteilernetzbetreiber im Sinne des Artikels 2 Nummer 29 der Richtlinie (EU) 2019/944
		— Übertragungsnetzbetreiber im Sinne des Artikels 2 Nummer 35 der Richtlinie (EU) 2019/944

Anhang I: 53 Arten

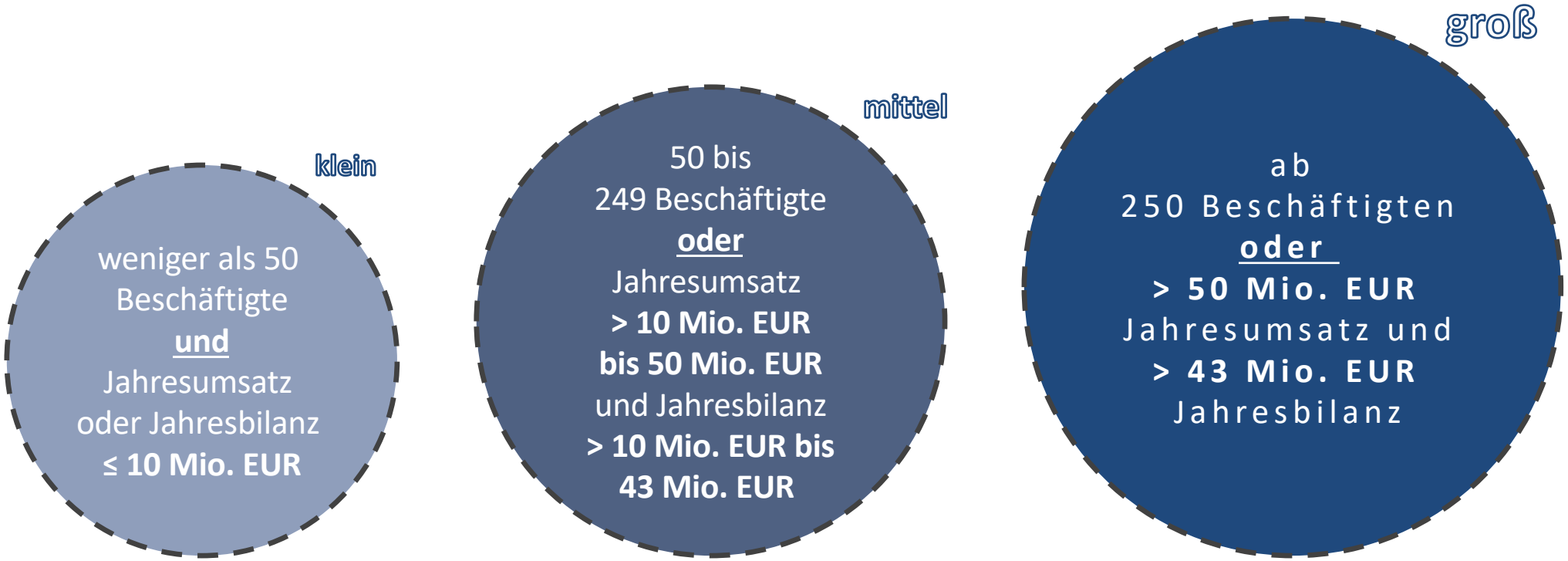
Anhang II: 14 Arten

SEKTOREN – WAS IST NEU GEGENÜBER NIS 1?

Anhang I (= Sektoren mit hoher Kritikalität)	Anhang II (= sonstige kritische Sektoren)
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 Produken und Geräten)	Verarbeitendes / Herstellendes Gewerbe (Medizinprodukte; Datenverarbeitungs-, elektronische und optische Geräte und elektronische Ausrüstungen; Maschinenbau; Kraftwagen und Kraftwagenteile und sonstiger Fahrzeugbau)
Trinkwasser	Anbieter digitaler Dienste (Suchmaschinen, Online-Marktplätze und soziale Netzwerke)
Abwasser	Forschung
Digitale Infrastruktur (IXP, DNS, TLD, Cloud-Computing, Rechenzentren, CDN, TSP und Anbieter öffentlicher elektronischer Kommunikationsnetze- und dienste)	
Verwaltung von IKT-Diensten (B2B)	
Öffentliche Verwaltung	
Weltraum	* **blau** = Neuerung gegenüber NIS1

UNTERNEHMENSGRÖSSE

Orientierung an Art 2 des Anhangs der **Empfehlung 2003/361/EG**



WESENTLICHE ODER WICHTIGE EINRICHTUNG (ANHANG I)?

Sektoren	Große Unternehmen	Mittlere Unternehmen	Kleinunternehmen
Anhang I			
Energie / Verkehr / Bankwesen / Finanzmarktinfrastrukturen / Gesundheitswesen / Trinkwasser / Abwasser / **Verwaltung von IKT-Diensten /** Weltraum	wesentlich	wichtig	

- Große Unternehmen — **Wesentlich**
- Mittlere Unternehmen — **Wichtig**
- Kleinunternehmen — grds. nicht im Anwendungsbereich
- Sonderregel — **Digitale Infrastruktur**

WESENTLICHE ODER WICHTIGE EINRICHTUNG (ANHANG II)?

Sektoren	Große Unternehmen	Mittlere Unternehmen	Kleinunternehmen
Anhang II			
Post- und Kurierdienste / Abfallbewirtschaftung / Lebensmittel / Verarbeitendes Gewerbes bzw. Herstellung von Waren / Anbieter digitaler Dienste / Forschung	wichtig	wichtig	

- Große Unternehmen — **Wichtig**
- Mittlere Unternehmen — **Wichtig**
- Kleinunternehmen — grds. nicht im Anwendungsbereich
- Sonderregel — **Digitale Infrastruktur**

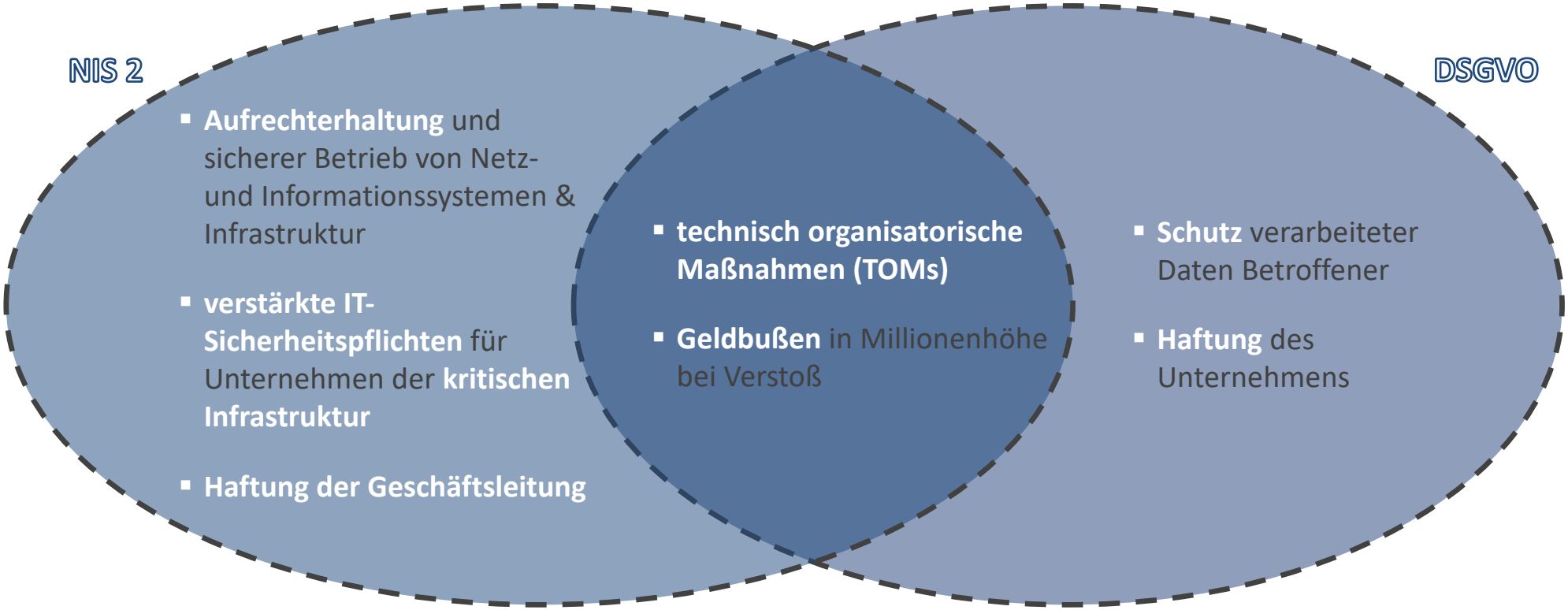
WAS IST JETZT ZU TUN? – RISIKOMANAGEMENTMASSNAHMEN

- **All-Gefahren-Ansatz**
- **Risikobasierter Ansatz**
  - technisch organisatorische und operative Maßnahmen
  - Ausmaß der **Risikoexposition** – Größe des Unternehmens
  - **Notfall- und Krisenmanagement** (Betriebskontinuität)
  - Kosten der Umsetzung und **Stand der Technik**

WAS IST JETZT ZU TUN? – RISIKOMANAGEMENTMASSNAHMEN

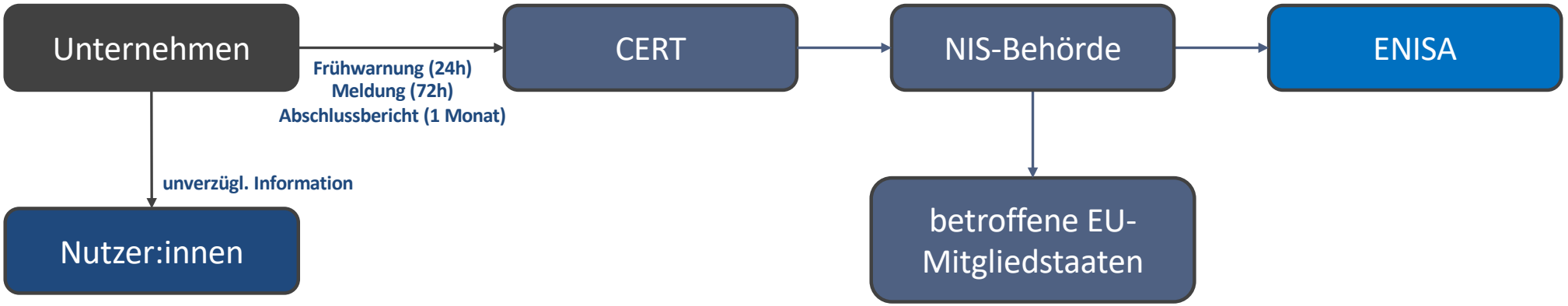
- Konzepte in Bezug auf die **Risikoanalyse** und Sicherheit für Informationssysteme
- **Bewältigung** von Sicherheitsvorfällen
- **Business Continuity** und Krisenmanagement
- **Lieferkettensicherheit**
- **Sicherheitsmaßnahmen** bei **Erwerb, Entwicklung und Wartung** von IKT
- Grundlegende Praktiken der **Cyberhygiene** und **Schulungen** zur Cybersicherheit
- Konzepte und Verfahren für den Einsatz von **Kryptografie** und ggf Verschlüsselung
- Sicherheit des **Personals**, Konzepte für die **Zugriffskontrolle**, **Mehrfaktor-Auth.**

BESONDERHEITEN NIS 2 – PARALLELEN & UNTERSCHIEDE DSGVO



BERICHTSPFLICHTEN

- Unternehmen müssen **erhebliche Sicherheitsvorfälle** unverzüglich an das **Computer-Notfallteam (CERT/CSIRT)** melden
- Unternehmen müssen gegebenenfalls **Empfänger** ihrer Dienste über erhebliche Sicherheitsvorfälle und Bedrohungen **informieren**



BERICHTSPFLICHTEN AM CERT

Frühwarnung

Frist: Unverzüglich bis max. 24 Stunden nach Kenntnisnahme	**Inhalt:** Verdacht, ob Sicherheitsvorfall auf rechtswidriger oder böswilliger Handlung beruht und ob grenzüberschreitend.

Meldung

Frist: Unverzüglich bis max. 72 Stunden nach Kenntnisnahme	**Inhalt:** Erste Bewertung des Sicherheitsvorfalls (inkl. Schweregrad, Auswirkungen, ggf Kompromittierungsindikatoren)

Abschlussmeldung

Frist: 1 Monat nach Meldung	**Inhalt:** Ausführliche Beschreibung, Angaben zur Art der Bedrohung, Ursachen, Abhilfemaßnahmen

AUFSICHT

- **Aufsichtsmaßnahmen und Befugnisse (ex ante und ex post)**
- **Mindestliste an Aufsichtsmaßnahmen** und Mitteln die den Behörden zur Verfügung stehen
  - **regelmäßige und gezielte Audits** (On- & Off-Site-Kontrollen, Sicherheitsscans)
  - **Ersuchen** um Informationen, **Zugang** zu Beweismitteln

DURCHSETZUNG

- Mindestliste an **Verwaltungssanktionen**
  - verbindliche **Anweisungen und Verwaltungsstrafen**
- **Maximale Bußgelder**
  - wesentliche Einrichtungen: **mind. 10 Mio EUR oder 2% des weltweiten Jahresumsatzes**
  - wichtige Einrichtungen: **mind. 7 Mio EUR oder 1,4% des weltweiten Jahresumsatzes**
  - **Haftung der Geschäftsleitung**

DISKUSSION

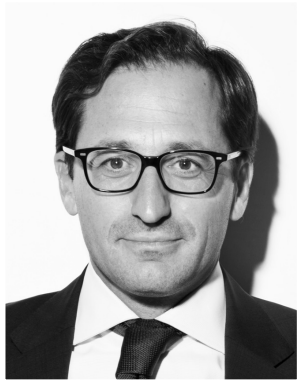
- **Erfahrungen**

- **Fragen**

aringer herbst winklbauer

Bundeskanzleramt

VIELEN DANK!



Dr. Stephan Winklbauer, LL. M.
Partner, Rechtsanwalt

aringer herbst winklbauer rechtsanwälte

Grillparzerstraße 5, 1010 Wien
+43 1 890 90 17
winklbauer@ahwlaw.at

www.ahwlaw.at

Ing. Clemens Möslinger, BA MSc

Bundeskanzleramt, Abteilung I/8
(Technologie- und Datenmanagement,
Cybersicherheit und Krisenrechenzentrum)

www.bundeskanzleramt.gv.at