Shecurity Masterclass · Block 3

Zwischen Anspruch und Anwendbarkeit

NIS2 · DORA · DSGVO · AI Act · Agentic AI

Bettina Sterner · kaffeekipferl.at · 4. Juli 2026

Agenda

Block 1

NIS2: Was übrig bleibt. Was dazukommt.

Block 2

KI im regulatorischen Kontext

Block 3

Agentic AI — Risiken & Recht

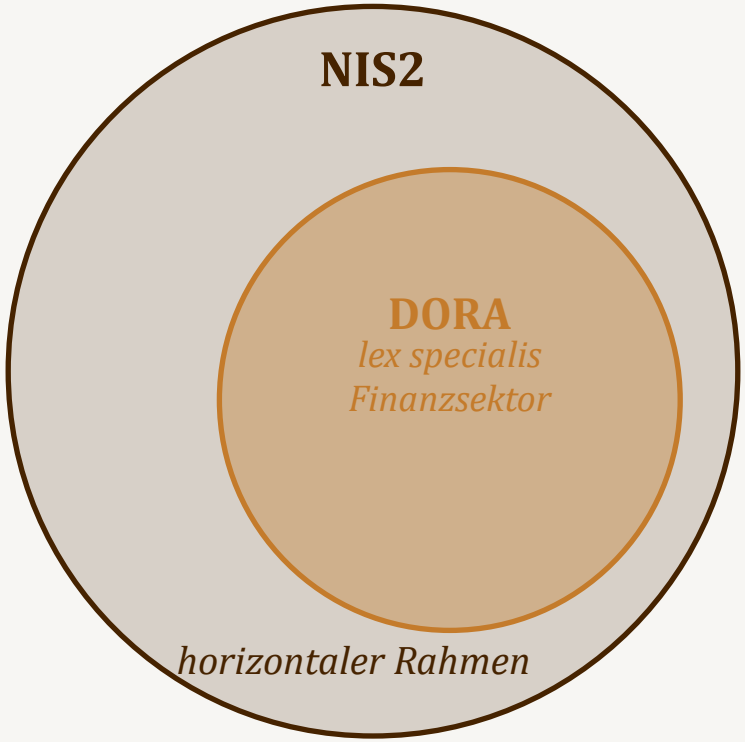
Block 4

Regulatorischer Ausblick

Block 1

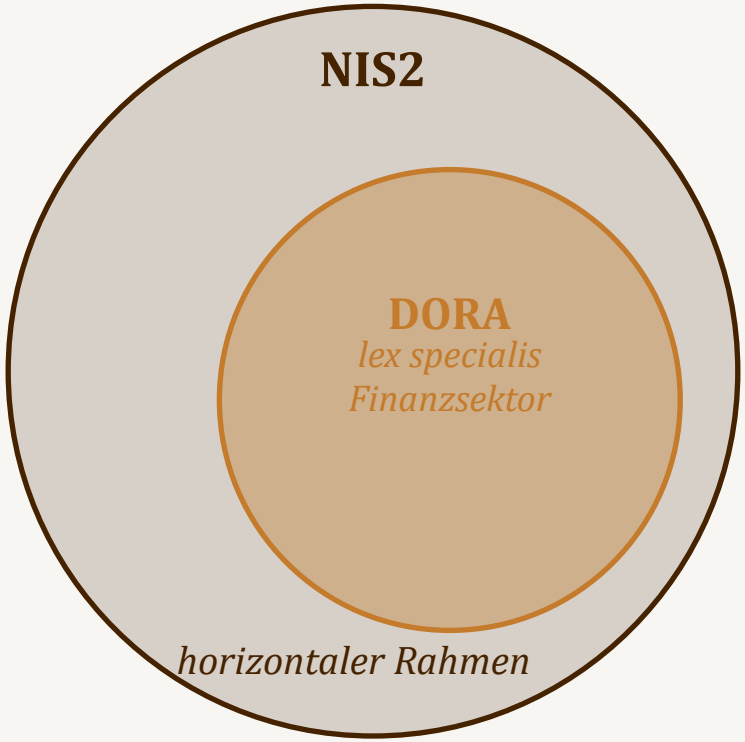
NIS2: Was übrig bleibt. Was dazukommt.

Das Verhältnis: Rahmen und lex specialis



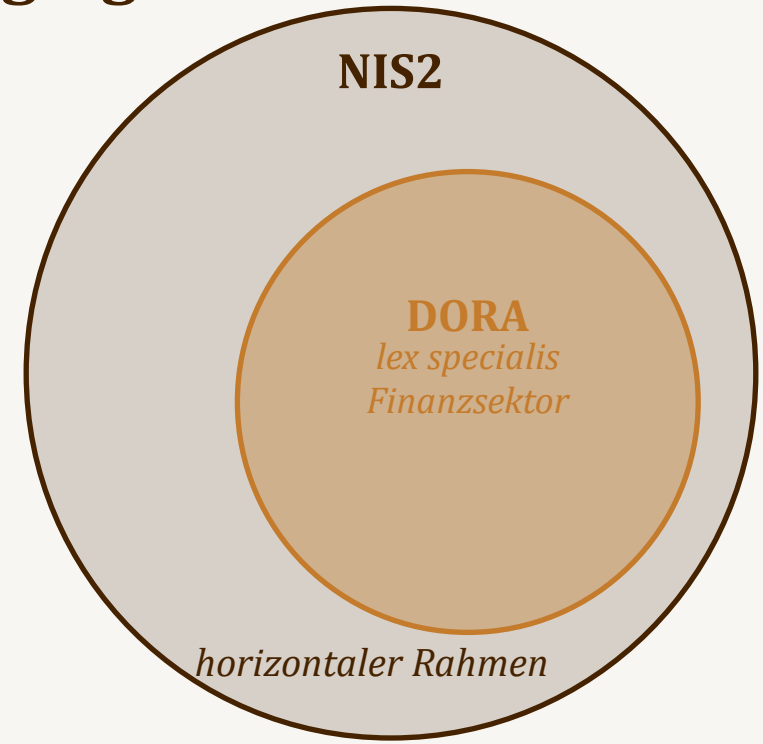
- **Im Finanzsektor: einzelne NISG-Pflichten weichen DORA**
- Außerhalb Finanzsektor: NIS2 ohne DORA-Overlay
- § 24 Abs. 7 NISG 2026:
  "Gegenüber Einrichtungen, die in den Anwendungsbereich der Verordnung (EU) 2022/2554 fallen, gehen die einschlägigen Bestimmungen dieser Verordnung und nationaler Durchführungsbestimmungen vor. Dies gilt auch für jene Einrichtungen, die gemäß Art. 2 Abs. 4 Verordnung (EU) 2022/2554 im Rahmen der innerstaatlichen Durchführung von deren Anwendungsbereich ausgenommen wurden."

Das Verhältnis: Rahmen und lex specialis



- „In sonstigen Konstellationen, in denen Finanzunternehmen dem Anwendungsbereich der DORA unterliegen, aufgrund ihrer konkreten Tätigkeit jedoch zugleich weiteren Sektoren nach Anlage 1 oder 2 zugeordnet werden können, finden DORA und NISG 2026 grundsätzlich nebeneinander Anwendung.“
- „In den Fällen, in denen DORA und das NISG 2026 nebeneinander anwendbar sind, wird es in praxi entsprechend enge Abstimmung und Zusammenarbeit zwischen Cybersicherheitsbehörde und DORA Behörde geben, um einen geregelten und effizienten Vollzug zu gewährleisten.“

Wo kann ich nachlesen, wenn mir das alles zu schnell ging?



- **Website FMA:** https://www.fma.gv.at/querschnittsthemen/dora/fma-aktivitaeten-zu-dora/ (Punkt "Informationen zum Verhältnis zwischen DORA und NIS2/NISG 2026 für Finanzunternehmen)
- **Check auch dort verfügbare Präsentation der FMA**

NIS2 vs. DORA: Was sie inhaltlich unterscheidet

NIS2 eigenständig

- Physische Sicherheit (Art. 21)
- Schwachstellenoffenlegung (Art. 12)
- **Sicherheit von Netz- und Informationssystemen**
- Sicherheit im Beschaffungsprozess

DORA eigenständig

- **Digitale operationale Resilienz** (4 Aspekte)
- TLPT als reguliertes Instrument
- CTPP-Designation (Art. 31)
- Informationsregister (Art. 28(3))
- Dezidierte Risikokontrollfunktionen (Art 5 Abs 3, Art 6 Abs 4), **3LoD-Modell**

Kurze Zusammenfassung

Bankwesen / Finanzmarktinfrastruktur	*Lex specialis: bestimmte NISG-Paragraphen gelten nicht*	FMA
DORA-Unternehmen auch in anderen NIS2-Sektoren tätig	*NISG 2026 gilt zusätzlich neben DORA*	FMA + NIS-Behörde
Finanzinstitut als IKT-Dienstleister für anderes Finanzinstitut (auch konzernintern)	*Führt NICHT zur Doppelanwendung DORA + NIS2*	FMA + NIS-Behörde
IKT-Drittdienstleister (kein Finanzunternehmen)	*NISG 2026 gilt neben DORA*	FMA + NIS-Behörde

NIS2-Eigenständigkeit im Detail

- Physische Sicherheit: explizit in Art. 21(2)(e)
- Koordinierte Schwachstellenoffenlegung (Art. 12)
- Meldepflicht an CERT/nationale Behörde
- Sicherheit im Beschaffungsprozess: Art. 21(2)(d)

Was NIS2 von DORA lernen kann

IKT Risk Management Framework

5 Säulen, konkret und messbar

Vertragsanforderungen

Art. 30: Granularität, Ausstiegsrecht

TLPT

Reguliertes Penetration Testing

CTPP-Oversight

Systemisches Risiko, direkte Aufsicht;
Konzentrationsrisiko

Leitungsorgan-Pflichten

DORA Art. 5: konkreter ausformuliert

Infosicherheitsziele

C/I/A/Authentizität — DORA explizit, NIS2 nicht

Was gerne übersehen wird: DSGVO bleibt eigenständig

„Sicherheitsmaßnahmen aufgrund der NIS-2-RL sind zwingend, doch ihre datenschutzkonforme Ausgestaltung bleibt eine eigenständige Pflicht. Eine pauschale „Sicherheitsklausel“ gibt es nicht, jede Verarbeitung benötigt eine tragfähige Rechtsgrundlage.“

Veronika Gelser, ZD 2026, 330

Integriert gedacht: NIS2 + DORA-Logik

- DORA-Granularität auch für NIS2-Drittanbieter nutzen
- **3 Lines of Defence-Modell**
- TLPT-Methodik auch ohne DORA-Pflicht anwenden
- Vier Infosicherheitsziele als gemeinsamen Rahmen setzen

Block 2

KI im regulatorischen Kontext

LLM-Anbieter im regulierten Umfeld

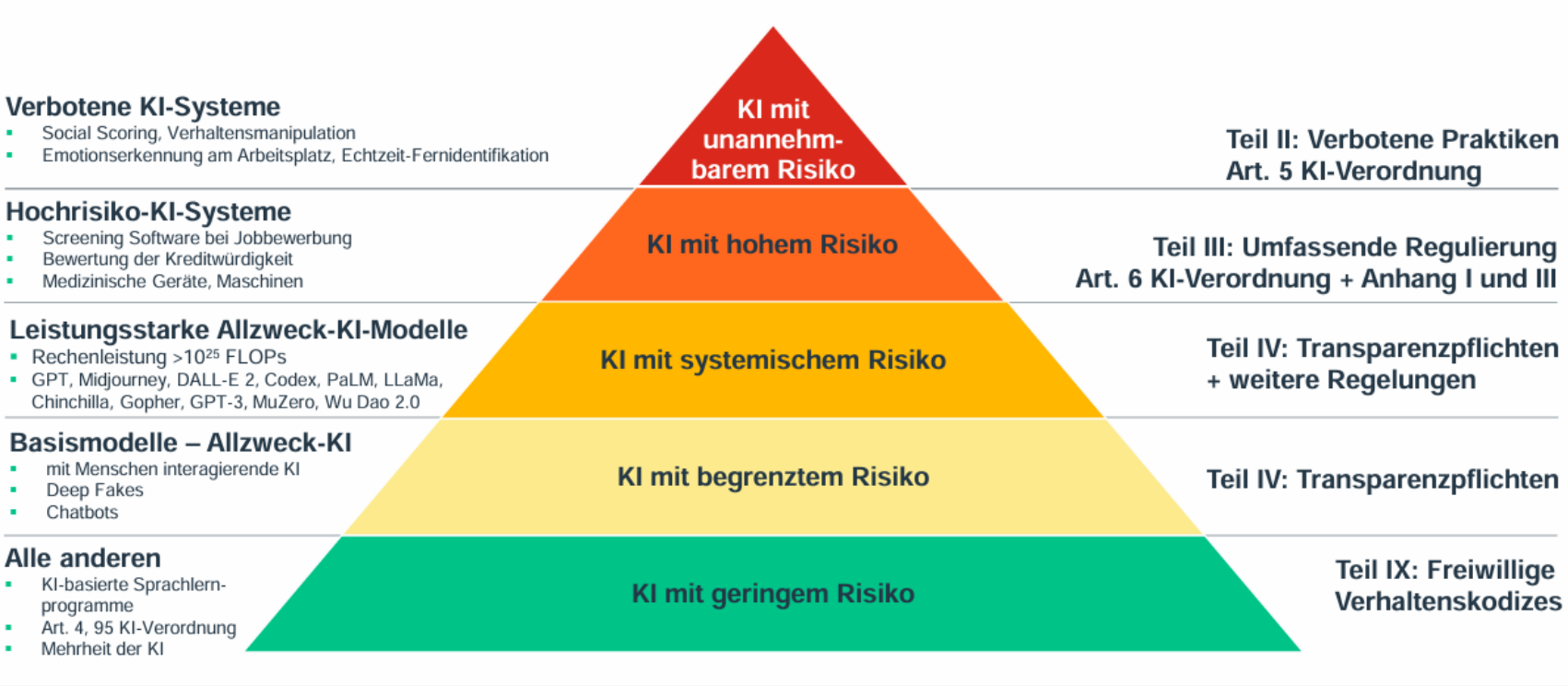
Kein kommerzieller Anbieter ist out-of-the-box DORA(oder NIS2)-compliant.

- Die Frage ist nicht: Welcher Anbieter ist compliant
- Sondern: Wo liegen die Gaps, wie groß, wie dokumentiert?
- US-Anbieter · Mistral · Llama on-premise

KI-VO + DORA/NIS2: Wo es “sich beißt”

- DORA: IKT-Risikomanagement für Finanzunternehmen
- NIS2: Sicherheit von Netz- und Informationssystemen für wesentliche und wichtige Einrichtungen
- KI-VO: Risikomanagement für KI-Systeme
- Ein KI-System bei einer betroffenen Einrichtung: alles gleichzeitig
- Risikoklassifikation folgen unterschiedlichen Logiken, keine “gegenseitige Anrechenbarkeit”

KI-VO: Risikoklassen



LLMs in der Praxis: Warum Governance relevant wird

Versicherungsmakler

ChatGPT für Kundenresearch → Kundendaten im Prompt

HR-Abteilung

KI für Bewerber*innen-Vorauswahl → Art. 22 DSGVO, Hochrisiko

Finanzberatung

LLM für Anlageempfehlung → Haftung

Rechtsabteilung

LLM für Vertragsanalyse → Art. 9 DSGVO möglich

Claude Mythos: Regulatorischer Weckruf

- 7. Apr `26: Anthropic kündigt Mythos & "Project Glasswing" an
- 7. Apr `26 : Krisensitzung FED & US-Treasury mit US-Bank-CEOs
- 13. Apr `26 : Mythos besteht AISI-Test "The last ones" als erstes Modell
- 30. Apr `26 : OpenAI GPT 5.5 zeigt vergleichbare Fähigkeiten im selben Test
- 2. Jun `26 : FMA / OenB-DORA Dialog

FMA-Stellungnahme Mai 2026: Erwartung ohne Maßstab

Die FMA erwartet, dass Finanzunternehmen aktuelle Empfehlungen zeitnah berücksichtigen. Einzige konkrete Handlungsempfehlung: **Table-Top-Übungen.**

Die eigentliche Frage, die kein Rechtsrahmen stellt: Wie lange ist eine Organisation blind — und was passiert in dieser Zeit?

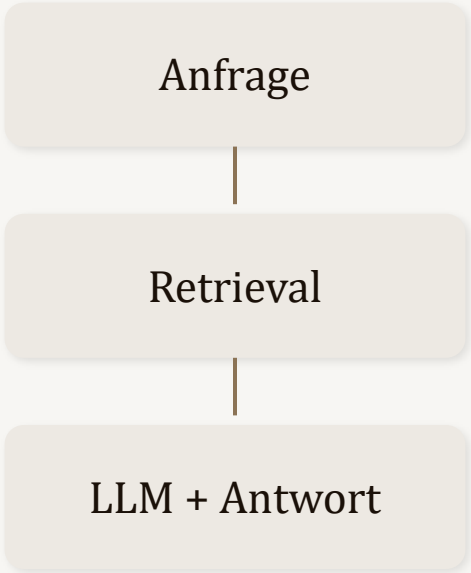
7 Tage
medianer Vorsprung der Angreifer nach CVE-Veröffentlichung
Mandiant/BSI BITS-B 2026

3,4 Std.
vom ersten Zugriff bis zum Active Directory-Durchgriff
Sophos Active Adversary Report 2026

Assume Breach
kein Zusatzmodul — ein Paradigmenwechsel

https://www.kaffeekipferl.at/publikationen -> Der 7-Tage-Vorsprung (WP)

Klassisches RAG: Das Grundmodell



Mensch steuert.
Mensch empfängt.
Kontrolle bleibt.

Agentische Systeme: Was sich fundamental ändert

- Autonome Planung
- Selbstinitiierte Tool-Aufrufe
- Iterative Reasoning-Schleifen
- Externalisierung in Umsysteme

Datenklassifizierung: Voraussetzung, keine Kür

- **Was darf das System "sehen"?**
- **Was darf es weitergeben?**
- **Was darf es in Umsysteme schreiben?**
- Ohne Klassifizierung: keine Zugriffskontrolle

Die “Lethal Trifecta”

Prompt Injection Vulnerability

Zugriff auf sensitive Ressourcen

Handlungsfähigkeit ohne Oversight

Kein Faktor allein ist das Killermerkmal.

Block 3

Agentic RAG — Risiken & Recht

DSGVO / Betroffenenrechte: Was bleibt, was bricht weg?

- Transparenz (Art 13, 14): Explainable AI
- Auskunft (Art. 15): Embeddings in Vektordatenbank
- Berichtigung (Art 16): Trainingsdaten nicht korrigierbar — Modellausgabe korrigierbar, Modell selbst nicht.
- Löschung (Art. 17): Quelle UND Vektordatenbank
- Widerspruch (Art. 21): Gegen autonome Entscheidungen
- Automatisierte Entscheidungen im Einzelfall einschließlich Profiling (Art 22)

DSGVO: Zweckbindung & faktische Steuerungsfähigkeit

- **Art. 5(1)(b) DSGVO: Zweckbindung**
- Zweck kann sich mid-execution ändern
- **Faktische Steuerungsfähigkeit als Haftungskriterium**
- Kill-Switch · Logging · Eingreifbarkeit

CLOUD Act & FISA 702: Das strukturelle Problem

> *"The obligation follows the provider, not the location."*

- EU-Datenresidenz schützt nicht vor US-Behördenzugriff
- FISA 702: re-autorisiert April 2024, erweiterter Scope
- PCLOB ohne Quorum seit Anfang 2025
- **NEU (29.6.2026): US Supreme Court, FTC nicht mehr unabhängig**

Art. 9 DSGVO & DPA Qualität von OpenAI (Beispiel)

- **OpenAI DPA: expliziter Art. 9-Ausschluss im Annex zum Data Processing Addendum, Stand Mai 2026** (≠ Art 28 DSGVO-Vereinbarung)
- TOMs nicht prüfbar: "industry best practices"
- Einseitige Änderungsrechte: Kündigung ≠ Governance
- Garante: 15 Mio. EUR gegen OpenAI (Dez. 2024)

Data Poisoning: Agentic-Systeme im Nachteil

- Klassisch: Vergiftung der Trainingsdaten
- Agentic: Vergiftung der Wissensbasis in Echtzeit
- Autonome Weiterverbreitung über Umsysteme
- Kaskade: Agent A vergiftet Wissensbasis von Agent B

Anthropic / UKASI / Alan Turing Institute · Oktober 2025 · arxiv.org/abs/2510.07192

Prompt Injection → Kontrollverlust

- Direkt: Manipulation des User-Inputs
- Indirekt: Vergiftete Dokumente im Retrieval
- Agentic: Injection triggert Tool-Aufrufe
- **Output-Problem → Aktions-Problem**

OWASP Top 10 für LLMs: Was es abdeckt

- LLM01: Prompt Injection
- LLM02: Unsicherer Output-Umgang
- LLM03: Trainingsdaten-Vergiftung
- LLM06: Übermäßige Berechtigungen
- LLM08: Vektorspeicher-Schwachstellen

Breit genutzt.
Stand der Praxis.

OWASP Top 10: Systematische Grenzen bei Agentic AI

- Entwickelt für statische LLM-Deployments
- Kein Modell für Multi-Agent-Interaktionen
- Agentische Angriffsvektoren fehlen weitgehend
- **OWASP Agentic Security Initiative**

Architektonische Mindestanforderungen

- Least Privilege für Tools
- Sandboxed Code Execution
- Human-in-the-Loop für irreversible Aktionen
- Audit-Trail aller Tool-Calls
- Netzwerk-Whitelisting (SSRF-Prävention)

Block 4

Regulatorischer Ausblick

NIS2-RL Proposal: Was sich ändert
(Spoiler: Nicht viel)

- COM(2026) 13 - Directive Proposal for simplifation measures and alignment with the Cybersecurity Act (veröffentlicht 21. Jänner 2026)
- Was sich ändern soll:
  - Anwendungsbereich: Präzisierungen und Erweiterungen
  - Neue Kategorien: Digital Identity Wallets, Business Wallets, Strategic Dual-Use Infrastructure, Submarine Data Transmission Infrastructure
  - Ransomware: Harmonisierte Datenerfassung (Angriffsvektor, Lösegeldstatus)
  - Lieferkette: Kommissionsleitlinien zur Vereinheitlichung — Entlastung, nicht Verschärfung
  - Post-Quantum-Kryptographie: Migrationspflicht in nationalen Cybersicherheitsstrategien
  - ENISA: Neue Koordinierungsrolle bei grenzüberschreitenden Einrichtungen
  - **Was fehlt: Stärkere Verzahnung der Regularien in Sachen KI (Beispiel CRA)**

Digital Omnibus in Sachen KI-VO

- **Digital Omnibus on AI:**
  - Fristverschiebung Hochrisiko-KI / Anhang III Gültigkeit auf 2. Dezember 2027
  - **Dh Fristen "neu":**
    Seit 2. Februar 2025 KI-Kompetenz und Verbotene Praktiken
    Ab 2. August 2026: Allgemeiner Geltungsbeginn KI-VO

    Hochrisiko-KI über Anhang III: 2. Dezember 2027
    Hochrisiko-KI über Produktsicherheit (Art 6 Abs 1 iVm Anhang I): 2. August 202
    Generative KI / maschinenlesbare Markierung: 2. Dezember 2026
    Transparenzpflicht nach Art 50 Abs 4: 2. August 2026
  - Delegierte Verordnung der Kommission für sektorspezifische Produktregelungen: 2. August 2027

Digital Omnibus in Sachen KI-VO

- **Digital Omnibus on AI - weitere relevante Änderungen**
  - Neue Verbotene Praktiken, gültig ab 2. Dezember 2026
  - Besondere Datenkategorien - erste und einzige Rechtsgrundlage für Verarbeitung pb Daten in der KI-VO!
  - Erleichterungen für KMUs

Cloud and AI Development Act (CADA)

- **Kommissionsvorschlag vom 3. Juni 2026,** Teil des EU Tech Sovereignty Package, reiner Draft-Status derzeit (COM(2026)502)
- ABER:
  - **“Frontier AI”** erstmals definiert - “means AI models or AI systems built upon such models that can perform a wide variety of tasks and that approach, **reach or exceed the current state of the art**“
  - **„AI Agent“ erstmals definiert** - „means an AI system or a coordinated set of AI systems, that can perceive and act upon their environment, with a degree of autonomy, using tools as needed to achieve specific goals and adapt to changing inputs and contexts“

Cloud and AI Development Act (CADA)

- **Cloud Sovereignty Framework:** Mit vier Assurance Levels für Cloud-Dienste (Anhang II)
- Zudem **politische / strategische Ziele**, zB Verdreifachung der EU-Rechenzentrumskapazität, geopolitische Dimension (Drittstaaten-Anbieter verpflichtend gegen EU Framework zu zertifizieren)
- **Mittel- bis längerfristig:** Öffentliche Stellen und NIS2-pflichtige Einrichtungen müssen Sovereignty Risk Assessment durchführen -> nach dem derzeitigen Stand (Juni 2026) US Hyperscaler auf Assurance Level 1 oder 2 -> im Ergebnis: Migration auf höher zertifizierte Anbieter oder dokumentierte Risikoakzeptanz mit Begründung

5 Key Messages

- **Agentic AI verändert Risikoarchitektur fundamental**
- **US Cloud Abhängigkeit als regulatorisches Risiko:** DPF, DORA, CADA
- **DSGVO eigenständig weiter gültig:** Auch bei NIS2 / DORA und KI-VO -> gleichzeitige Compliance gewährleisten - interdisziplinäre Teams
- **Kein kommerzieller LLM Anbieter out of the box compliant**
- **Regulatorischer Rahmen ist im Umbau**

Danke.

Bettina Sterner · kaffeekipferl.at · https://www.linkedin.com/in/bettina-sterner-45430717b/