HERZLICH WILLKOMMEN

WIE WAPPNEN WIR UNS FÜR DIE EUROPÄISCHE DIGITALSTRATEGIE?

Europäische Cyberstrategie| europäische Datenstrategie

Mag. Katharina Raabe-Stuppnig & *Dr. Maria-Luise Fellner*

INHALTSVERZEICHNIS

WOVOR WAPPNEN? — „Digitalstrategie“:

Datenstrategie, Cybersecurity-Strategie, AI-Strategie...

ÜBERBLICK — Ausgewählte EU-Rechtsakte im Überblick

CHALLENGES — Ausgewählte Beispiele

WIE WAPPNEN? — Gedanken zur effektiven Vorbereitung auf die (legislative) digitale Dekade der EU

WOVOR GILT ES SICH ZU WAPPNEN?

Cyber-Security in einem erweiterten Kontext...

WOVOR WAPPNEN?

"The Commission is determined to make this Europe's "Digital Decade".
Europe must now strengthen its digital sovereignty and set standards, rather than following those of others – with a clear focus on data, technology, and infrastructure." ("Europe fit for the digital age")

DIGITALSTRATEGIE

Strategische Ziele:

A. Förderung einer digitalen Kultur

B. Ermöglichung einer digitaltauglichen EU-Politikgestaltung

C. Ermöglichung eines geschäftsorientierten digitalen Wandels

D. Gewährleistung einer nahtlosen digitalen Landschaft

E. Erhaltung einer grünen, sicheren und widerstandsfähigen Infrastruktur

DATENSTRATEGIE

A. Sektorübergreifender Governance-Rahmen für den Datenzugriff und die Datennutzung

B. Voraussetzungen: Investitionen in Daten und in die Stärkung der europäischen Kapazitäten und Infrastrukturen für das Hosting, die Verarbeitung und die Nutzung von Daten sowie der Interoperabilität

C. Stärkung der Handlungskompetenz des Einzelnen, Investitionen in Kompetenzen und in KMU

D. Gemeinsame europäische Datenräume in strategischen Sektoren und Bereichen von öffentlichem Interesse

CYBERSECURITY-STRATEGIE

Globales und offenes Internet mit starken Schutzmechanismen durch 3 Bereiche von EU-Maßnahmen:

1. Widerstandsfähigkeit, technologische Souveränität und Führung

2. Operative Kapazitäten zur Prävention, Abschreckung und Reaktion

3. Zusammenarbeit zur Förderung eines globalen und offenen Cyberspace.

AUSGEWÄHLTE RECHTSAKTE IM ÜBERBLICK

DMA
Digital Markets Act

DSA
Digital Services Act

DGA
Data Governance Act

NIS2
Network and Information Security 2

DORA
Digital Operational Resilience Act

DA
Data Act

CRA
Cyber Resilience Act

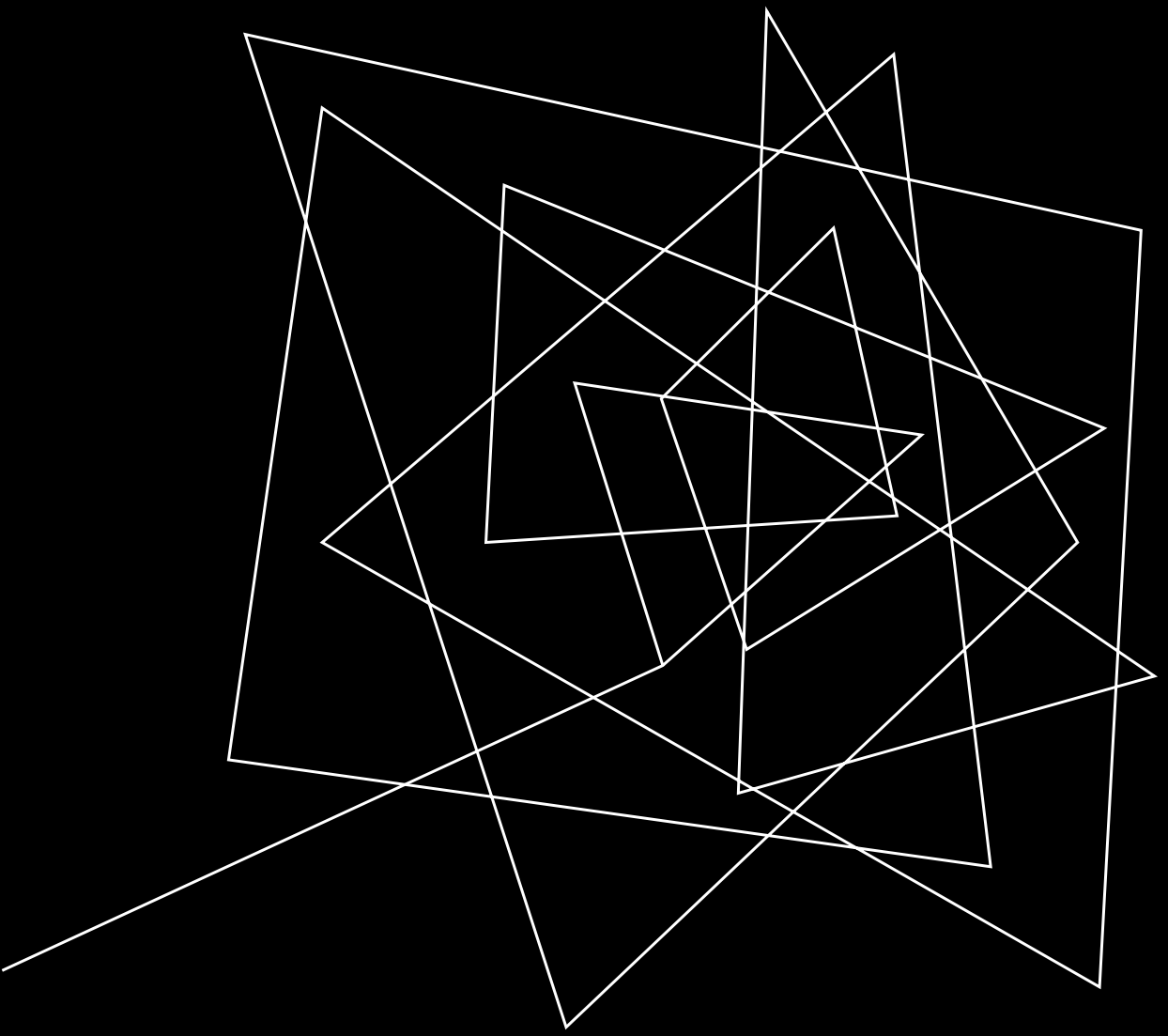
AIA
AI Act

AILD
AI Liability Directive

PLD
Product Liability Directive

AUSGEWÄHLTE RECHTSAKTE IM ÜBERBLICK

VO Digital Markets Act (DMA)	Wirksam seit 02.05.2023
VO Digital Services Act (DSA)	Wirksam ab 17.02.2024
VO Data Governance Act (DGA)	Wirksam ab 24.09.2023
RL über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS2)	Umsetzungsfrist für MS bis 17.10.2024
VO über die digitale operationale Resilienz im Finanzsektor (DORA)	Wirksam ab 17.01.2025
VO Data Act (DA)	Trilog seit 03/2013, Verabschiedung geplant 2023, 12 (24?) Mo bis Geltungsbeginn
VO Cyber Resilience Act (CRA)	Start Trilog voraussichtlich nicht vor Q3/2023, Verabschiedung ?, 24 Mo bis Geltungsbeginn
VO AI Act (AIA)	Trilog seit 06/2023, Verabschiedung geplant 2023, 24 Mo bis Geltungsbeginn
RL AI Liability Directive (AILD)	Start Trilog voraussichtlich nicht vor Ende/23, Verabschiedung ?, 24 Mo Umsetzungsfrist
RL Product Liability Directive (PLD)	Start Trilog voraussichtlich 10/2023, 12 (24?) Mo Umsetzungsfrist



RICHTLINIE ÜBER MAßNAHMEN FÜR EIN HOHES GEMEINSAMES CYBERSICHERHEITS-NIVEAU IN DER UNION (NIS2)

RL (EU) 2022/2555

In Kraft seit 16. Jänner 2023
Umsetzungsfrist 17. Oktober 2024

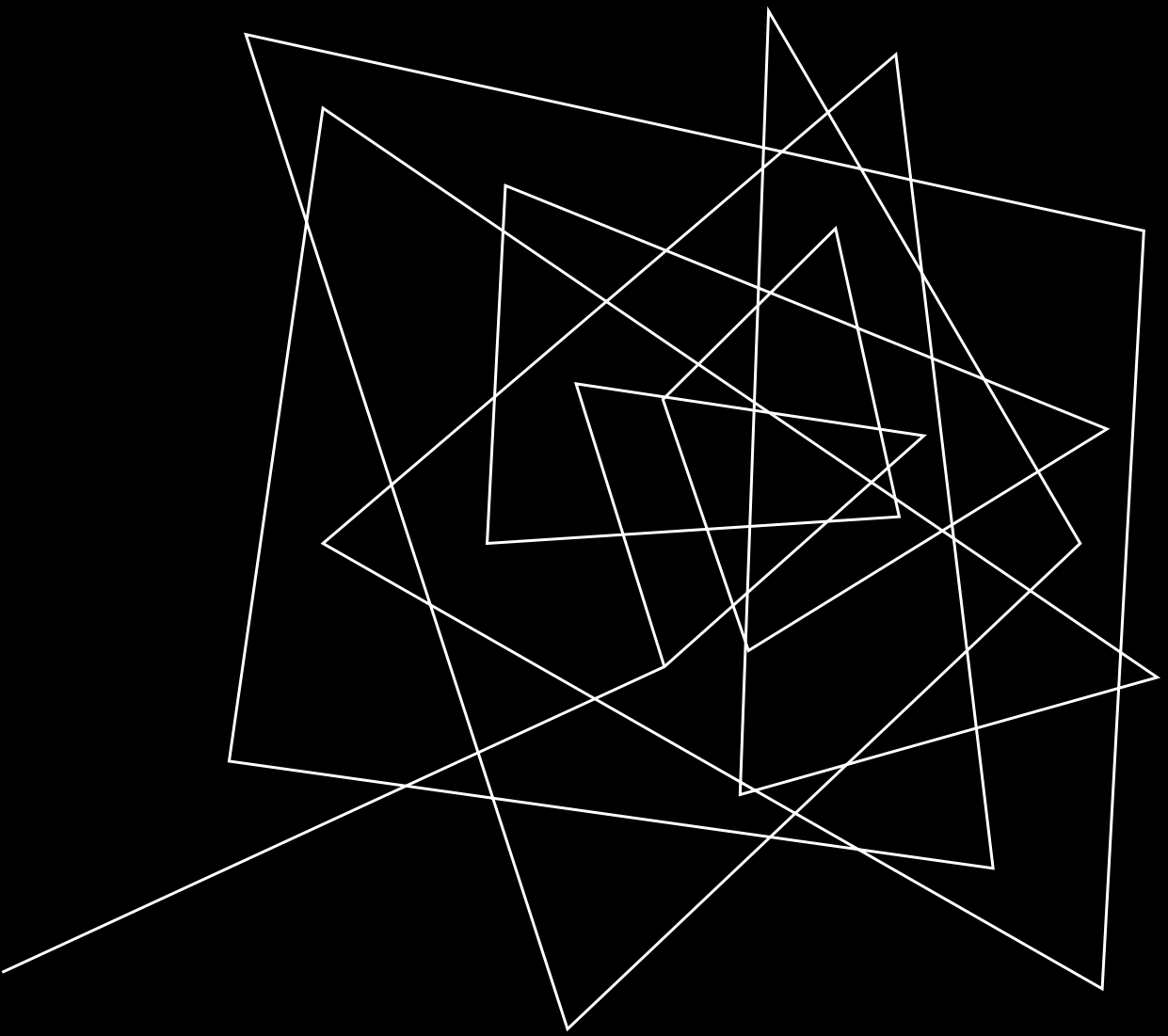
RICHTLINIE ÜBER MAßNAHMEN FÜR EIN HOHES GEMEINSAMES CYBERSICHERHEITSNIVEAU IN DER UNION (NIS2)

- **Wer ist betroffen?**
  - Große und mittlere Unternehmen kritischen Infrastruktur 18 Sektoren (ab 50 Mitarbeitern und 10 Mio Umsatz)
  - Unabhängig von der Größe:
    - i) Anbietern von öffentlichen elektronischen Kommunikationsnetzen oder von öffentlich zugänglichen elektronischen Kommunikationsdiensten;
    - ii) Vertrauensdiensteanbietern;
    - iii) Namenregistern der Domäne oberster Stufe und Domänennamensystem-Diensteanbietern;
    - Einziger Anbieter eines wesentlichen Dienstes
  - Zusätzlich müssen auch Dienstleister und Lieferanten von betroffenen Unternehmen Sicherheitsvorkehrungen einhalten
- **Worum geht es?**
  - Sicherung eines hohen gemeinsamen Cybersicherheitsniveaus in der EU
  - Grundlage für Risikomanagementmaßnahmen und Meldepflichten im Bereich Cybersicherheit

RICHTLINIE ÜBER MAßNAHMEN FÜR EIN HOHES GEMEINSAMES CYBERSICHERHEITSNIVEAU IN DER UNION (NIS2)

- **Richtlinien Umsetzung**
  - Frist 17. Oktober 2024
  - Österreichische Umsetzung?

- **Sanktionen:**
  - Bei Nichterfüllung drohen Sanktionen bis zu EUR 10 Mio und 2% des Gesamtjahresumsatzes des Konzerns
  - bei wesentlichen Einrichtungen bzw. EUR 7 Mio und 1,4% des Gesamtjahresumsatzes des Konzerns bei wichtigen Einrichtungen.



CYBER RESILIENCE ACT (CRA)

COM(2022) 454 final

- Trilog wahrscheinlich nicht vor Ende 2023,
- Verabschiedung (?);
- Geltung (weitestgehend) erst 24 Mo nach Verabschiedung

CYBER RESILIENCE ACT (CRA)

- **Wer ist betroffen?**
  - Hersteller, Importeure und Händler von Produkten mit digitalen Elementen

"Produkt mit digitalen Elementen" = Soft- oder Hardwareprodukte und deren Datenfernverarbeitungslösungen, inkl. Soft- und Hardwarekomponenten, die getrennt in Verkehr gebracht werden sollen.

Kritische Produkte mit digitalen Elementen (birgt Cybersicherheitsrisiko): unterliegen besonderen Konformitätsbewertungsverfahren und werden anhand des von ihnen ausgehenden Cybersicherheitsrisikos gemäß Anhang III in Klassen I und II unterteilt (Klasse II stellt ein höheres Risiko dar – hier muss zwingend ein Dritter in die Konformitätsbewertung des Herstellers miteinbezogen werden).

CYBER RESILIENCE ACT (CRA)

- **Worum geht es?**
  - Einführung gemeinsamer Cybersicherheitsvorschriften für Produkte mit digitalen Elementen
  - Insb. Vorschriften für grundlegende Anforderungen an Konzeption, Entwicklung und Herstellung sowie an Verfahren zur Behandlung von Schwachstellen, um die Cybersicherheit von Produkten mit digitalen Elementen während ihres gesamten Lebenszyklus zu gewährleisten.
  - Konformitätsbewertungsverfahren
  - Strategien und Verfahren zur Behebung von Schwachstellen
  - Meldepflichten gegenüber ENISA (unverzüglich, jedenfalls 24h ab Kenntnis: jede aktiv ausgenutzte Schwachstelle; Vorfall, der sich auf Sicherheit des Produkts auswirkt)
- **Ziele:**
  - Verbesserung der Sicherheit von IoT-Produkten für Verbraucher
  - Gewährleistung eines kohärenten Cyber-Sicherheitsrahmens, der Einhaltung der Vorschriften für Hard- und Softwarehersteller erleichtert
  - Verbesserung der Transparenz der Cyber-Sicherheitseigenschaften von Produkten mit digitalen Elementen

CYBER RESILIENCE ACT (CRA)

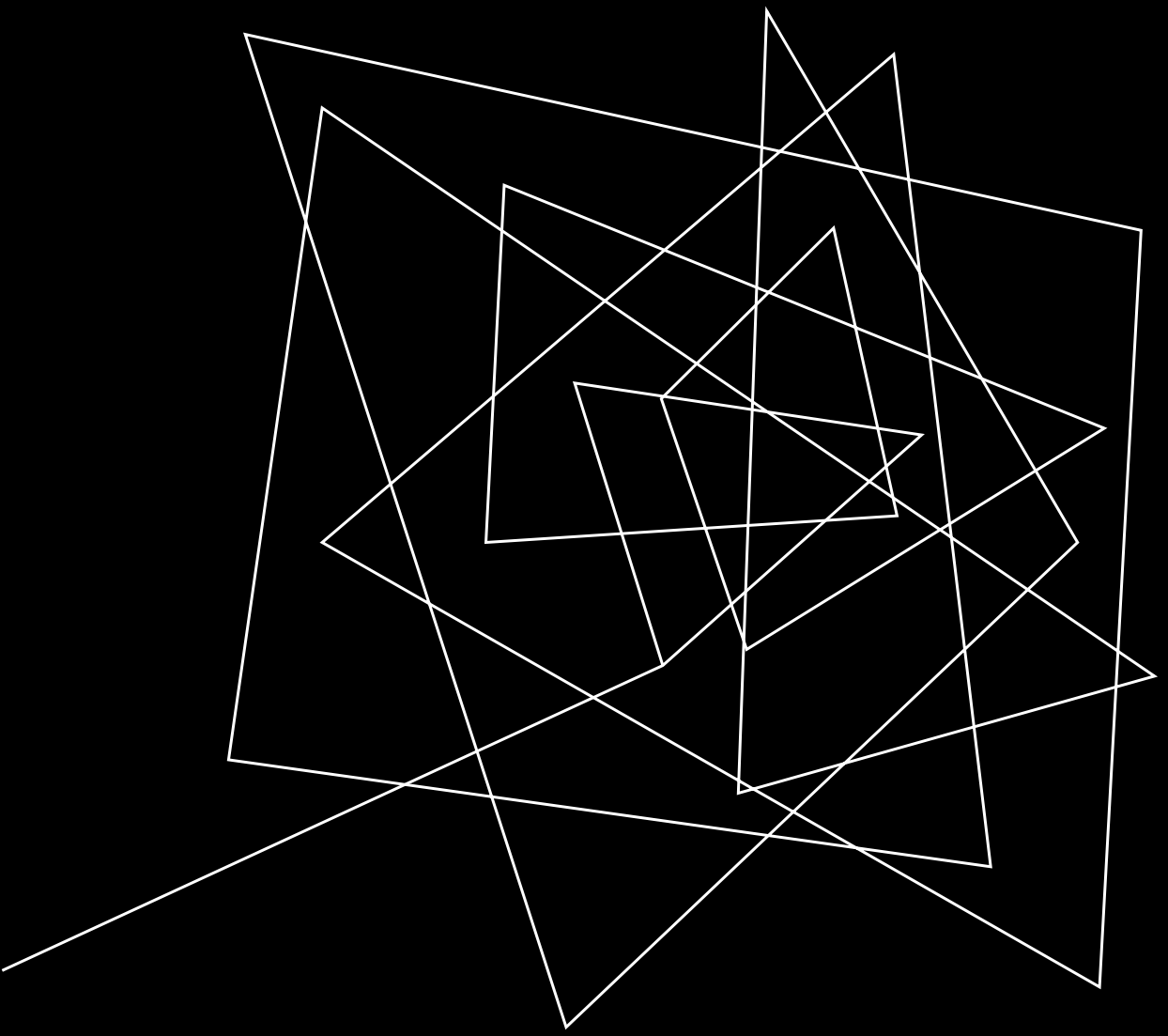
- **Konformitätsvermutung**
- Bei Produkten mit digitalen Elementen, die mit harmonisierten, im EU Amtsblatt veröffentlichten Normen übereinstimmen, wird Konformität mit CRA Anforderungen vermutet.

- **Bedeutung des CRA? | Was ist zu tun?**

1. Anwendbarkeit des CRA prüfen
   - Handelt es sich um ein (kritisches) Produkt mit digitalen Elementen?
2. Einordnung in Risikoklasse

CYBER RESILIENCE ACT (CRA)

- **Bestandsschutz für bestehende Produkte (Art 55)?**
- EU-Baumusterprüfbescheinigungen und Zulassungen nach anderen EU-Harmonisierungsrechtsvorschriften 42 Monate nach Inkrafttreten gültig
- Verbindlich für bestehende Produkte mit digitalen Elementen nur dann, wenn im Hinblick auf das Produkt nach Wirksamkeit des CRA die Konzeption oder Zweckbestimmung wesentlich geändert wurde.
- **Sanktionen:**
- Bei Nichteinhaltung der grundlegenden Cybersicherheits-anforderungen oder Nichteinhaltung der (Melde)Pflichten des Herstellers:
  - Geldbußen bis zu EUR 15 Mio. bzw 2,5% des gesamten weltweiten Jahresumsatzes.
- Bei Nichteinhaltung anderer Pflichten:
  - Geldbußen bis zu EUR 10 Mio bzw 2% des gesamten weltweiten Jahresumsatzes



AI ACT (AIA)

COM(2021) 206 final

- Trilogverhandlungen seit 06/2023;
- Verabschiedung für 2023 geplant (?)
- Wirksamkeitsbeginn 24 Monate nach Inkrafttreten

AI ACT (AIA)

- **Wer ist betroffen?**
  - Entwickler, Anwender und Nutzer von KI in der EU und Unternehmen aus Nicht-EU-Ländern, die KI-Systeme auf den Markt bringen oder in Betrieb nehmen oder deren Systeme in der EU verwendete Ergebnisse erzeugen.

- **Worum geht es?**
  - Rahmen von Anforderungen und Verpflichtungen für Entwickler, Anwender und Nutzer KI
  - Behördliche Aufsicht
  - Risikoklassifizierungssystem für KI

AI ACT (AIA)

- **Bedeutung des AIA? | Was ist zu tun?**

1. Anwendbarkeit des AIA prüfen
   - Handelt es sich um ein KI-System gem dem AIA

2. Einordnung in Risikogruppe
   a) Unannehmbares Risiko
   b) Hohes Risiko
   c) Geringes Risiko

AI ACT (AIA)

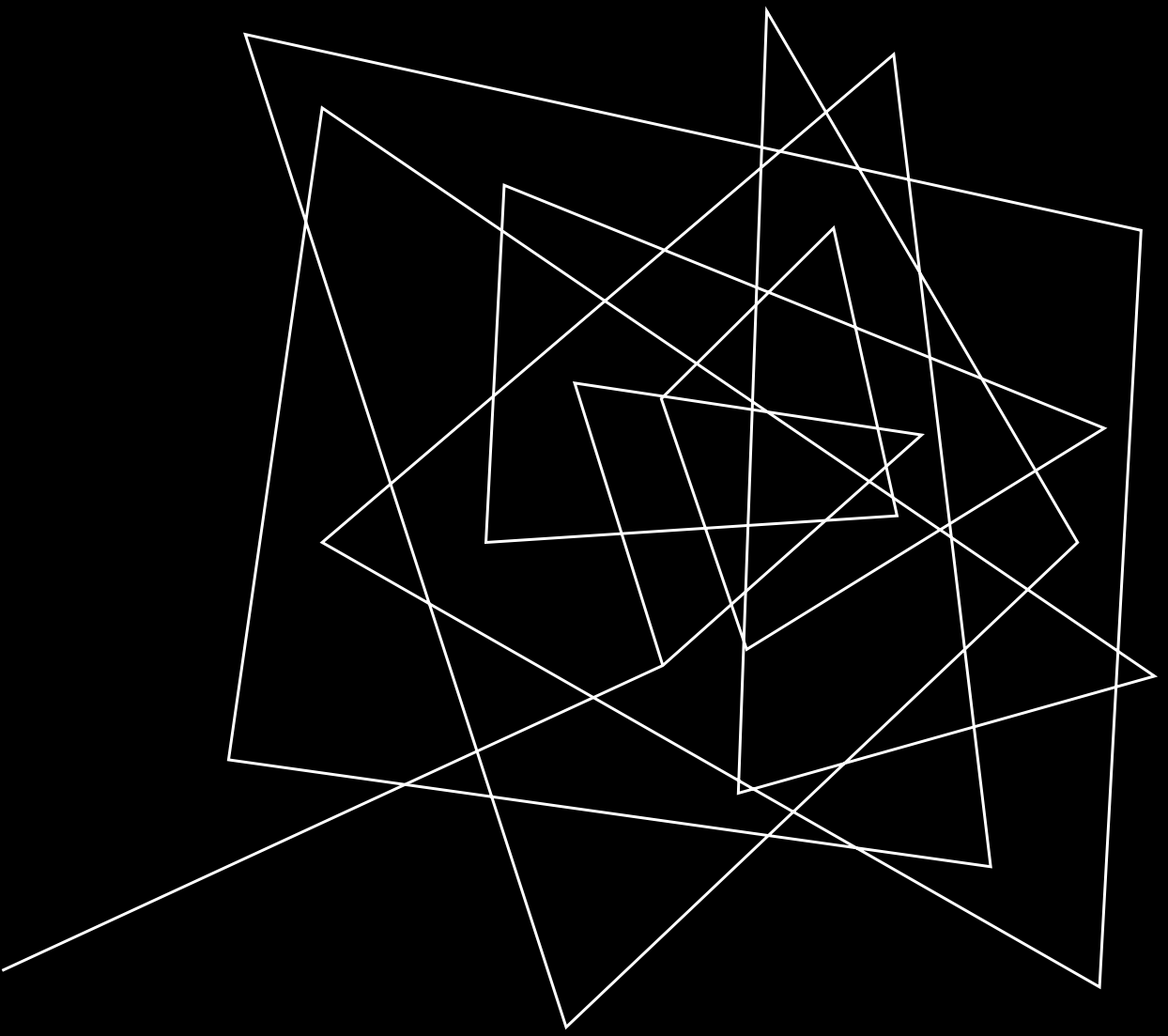
- **Bestandsschutz für bestehende Produkte (Art 83)**

Im Kommissionsvorschlag vorgesehen für

- Komponenten von IT-Großsystemen in Zusammenhang mit Rechts- und Sicherheitssystemen, die innerhalb von 12 M nach Anwendung der VO in Verkehr gebracht werden
- Bei Hochrisiko-KI-Systemen wenn sie vor Anwendung der VO in Verkehr gebracht wurden und in ihrer Konzeption und Zweckbestimmung nicht geändert werden.

- **Sanktionen:**

- Je nach Art des Verstoßes Bußgeld bis zu 30 Mio EUR oder 6% des weltweiten Jahresumsatzes



AI LIABILITY DIRECTIVE (AILD)

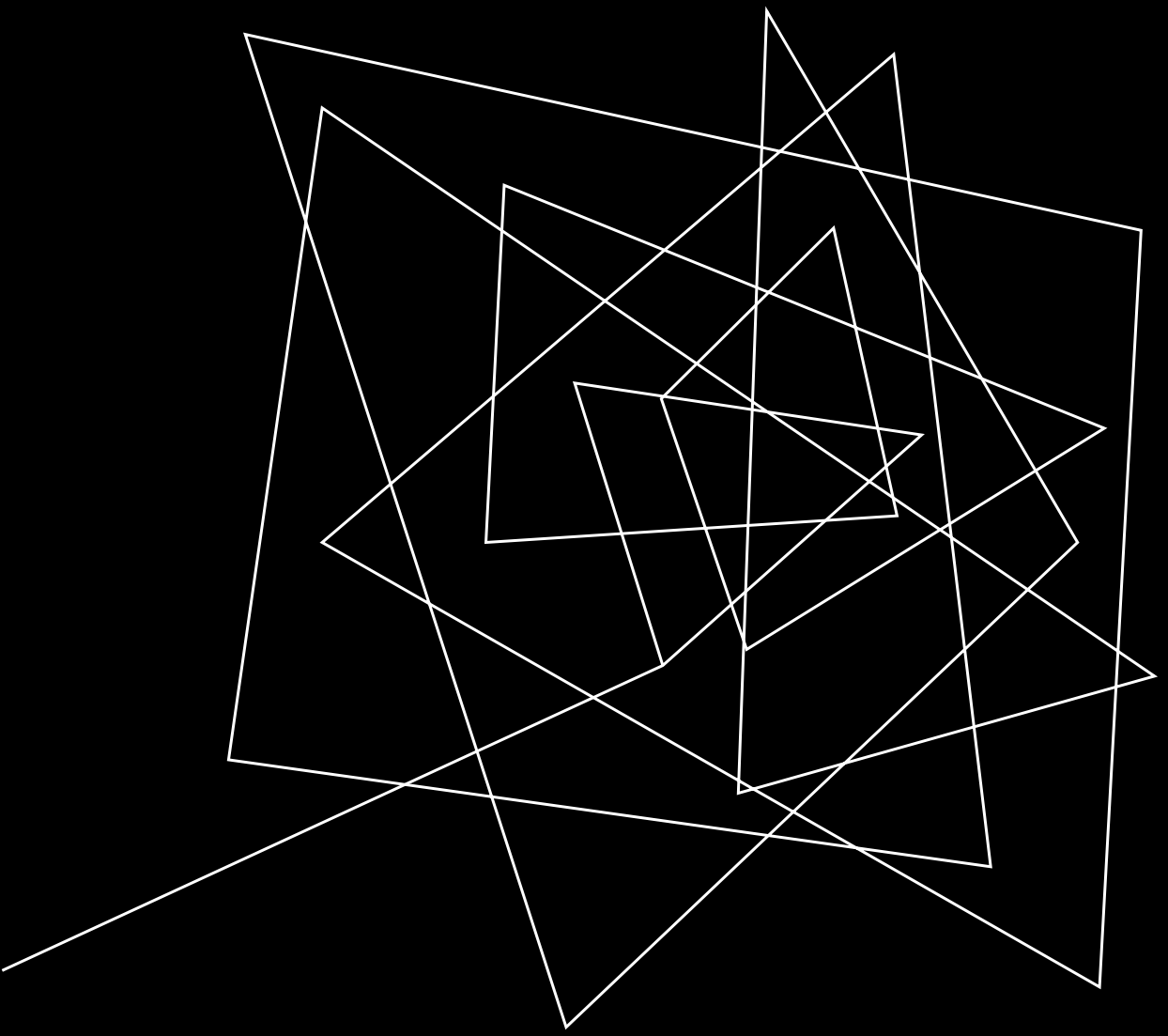
COM(2022) 496 final

Erster Vorschlag wurde im September 2022 veröffentlicht
Richtlinie ist binnen 2 Jahren umzusetzen

AI LIABILITY DIRECTIVE (AILD)

- **Wer ist betroffen?**
  - Hersteller und Anbieter von Kl-Produkten und –Dienstleistungen

- **Worum geht es?**
  - Harmonisierung der Haftung für KI
  - Erleichterter Zugang zu Schadenersatz für Opfer von KI-Schäden
    - Außervertraglicher verschuldensabhängiger zivilrechtlicher Anspruch auf Ersatz des Schadens, der durch ein Ergebnis eines KI-Systems oder aber dadurch, dass dieses System das von ihm erwartete Ergebnis nicht hervorgebracht hat, verursacht wurde;
  - Verfolgbarkeit von Verstößen gegen die Privatsphäre oder Sicherheitsaspekte



PRODUCT LIABILITY DIRECTIVE (PLD)

COM (2022) 0495 final

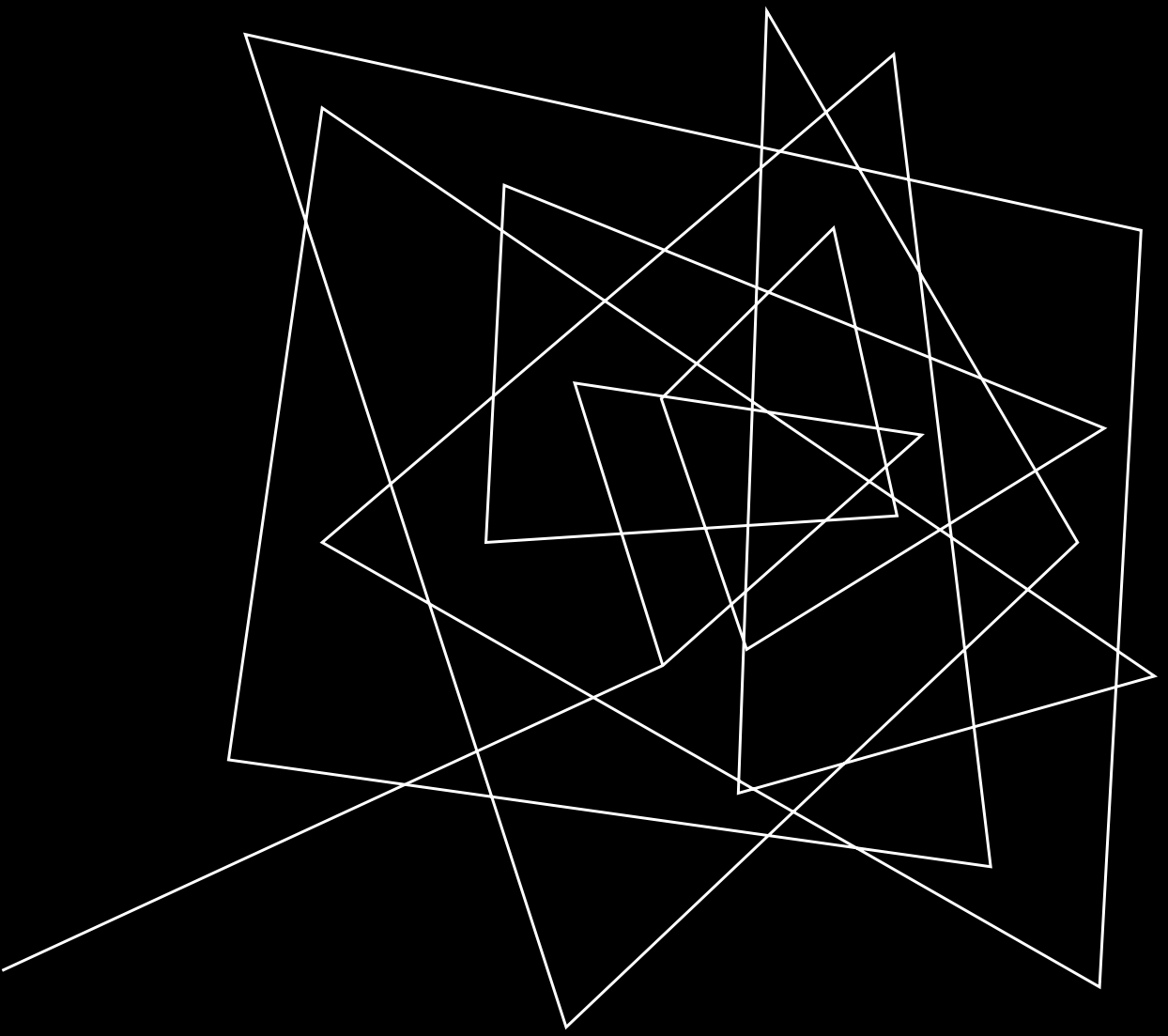
- Abstimmung im EU Parliament Committe für 07/2023 geplant
- Trilog könnte 10/2023 starten
- Inkrafttreten (?)
- Umsetzungsfrist für Mitgliedsstaaten: [12 (Kom) / 24] (Kompromissvorschlag Rat)

PRODUCT LIABILITY DIRECTIVE (PLD)

- **Wer ist betroffen?**
  - Hersteller von Produkten, Händler, Importeure;
  - Hersteller digitaler Dienste, die so in ein Produkt integriert oder so mit ihm verbunden sind, dass das Produkt ohne ihn eine oder mehrere seiner Funktionen nicht ausführen könnte.

- **Worum geht es?**
  - Verschuldensunabhängige Gefährdungshaftung für fehlerhafte Produkte
  - Software ist nun explizit Produkt iSd Richtlinie
  - Als Schaden gilt auch Verlust oder Verfälschung von Daten, die nicht ausschließlich für berufliche Zwecke verwendet werden;
  - Ein Produkt gilt als fehlerhaft, wenn es nicht die Sicherheit bietet, die die breite Öffentlichkeit erwarten darf, insb. auch betreffend Sicherheitsanforderungen einschließlich Cybersicherheitsanforderungen;
  - Erleichterung der Beweislast für Kläger
  - Aufhebung der Beschränkungen für Schadenersatzansprüche mit geringem Wert

- **Bestandsschutz (Art 2):**
  - Geltung für Produkte, die [12 / 24] Monate nach Inkrafttreten in Verkehr gebracht werden



DATA ACT (DA)

2022/0047 (COD)

- Trilogverhandlungen seit 03/2023;
- Verabschiedung für 2023 geplant (?)
- Wirksamkeitsbeginn 12 (24?) Monate nach Inkrafttreten

DATA ACT (DA)

- **Wer ist betroffen?**
  - Hersteller von (smarten) Produkten und Erbringer verbundener Dienste, die in der EU in Verkehr gebracht werden,
  - Dateninhaber und Datenempfänger,
  - öffentliche Stellen und Organe, Einrichtungen der EU,
  - Anbieter von Datenverarbeitungsdiensten.

"Produkt" = körperlicher beweglicher Gegenstand (der in einem unbeweglichen Gegenstand enthalten sein kann), der Daten über seine Nutzung oder Umgebung erlangt, erzeugt oder sammelt und Daten über einen öffentlich zugänglichen elektronischen Kommunikationsdienst übermitteln kann und dessen Hauptfunktion nicht die Speicherung und Verarbeitung von Daten ist.

"Verbundener Dienst" = digitaler Dienst (inkl Software), der so in ein Produkt integriert bzw damit verbunden ist, dass das Produkt ohne ihn eine seiner Funktionen nicht ausführen könnte.

„***Datenverarbeitungsdienst***“ = eine digitale Dienstleistung, bei der es sich um keinen Online-Inhaltedienst im Sinne des Artikels 2 Absatz 5 der Verordnung (EU) 2017/1128 handelt, die einem Kunden bereitgestellt wird und eine Verwaltung auf Abruf und einen breiten Fernzugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer, zentralisierter, verteilter oder hochgradig verteilter Rechenressourcen ermöglicht

DATA ACT (DA)

- **Worum geht es?**
- Daten iSd DA?
  - personenbezogene und nicht personenbezogene Daten
- Datenweitergabepflichten / Zugangsrechte B2C und B2B: für Daten, die der Nutzer durch Produkte oder verbundene Dienste erzeugt, die er besitzt, mietet oder least;
  - Nutzer kann Weitergabe an Dritte verlangen
  - Erlangte Daten dürfen nicht zur Entwicklung eines im Wettbewerb stehenden Produktes verwendet werden
- Bereitstellung von Daten für öffentliche Stellen wegen außergewöhnlicher Notwendigkeit;
- Wechsel zwischen Datenverarbeitungsdiensten;
- Schutzvorkehrungen für nicht personenbezogene Daten im internationalen Umfeld;
- Interoperabilitätsvorgaben.

DATA ACT (DA)

- **Bedeutung des DA? | Was ist zu tun?**

1. Anwendbarkeit des DA prüfen

- Produkt / verbundener Dienst?

2. Einordnung in die „Rollen“ des DA
   a) Dateninhaber
   b) Nutzer
   c) Datenempfänger?
   d) Strategie? Verpflichteter, Nutznießer?

DATA ACT (DA)

- **Bestandsschutz für bestehende Produkte / Verträge (Art 42)?**
  - Im Kommissionsvorschlag nicht vorgesehen
  - In der Verhandlungsposition des Rats angedacht:
    - Verbindlichkeit von Art 3 (direkter Datenzugriff des Nutzers) für Produkte, die 12 (?) Mo nach Wirksamkeit der VO in Verkehr gebracht werden
    - Verbindlichkeit für Verträge über Datenzugang erst nach Wirksamwerden der VO

- **Sanktionen**
  - Bei Verstößen gegen die Pflichten der Kapitel II, III und V sind die Datenschutzbehörden innerhalb ihres Zuständigkeitsbereichs befugt Geldbußen im Einklang mit Artikel 83 DSGVO zu verhängen (bis zu EUR 20 Mio. bzw 4% des gesamten weltweit erzielten Jahresumsatzes)

CHALLENGES

Ausgewählte Beispiele

SPANNUNGSVERHÄLTNISSE

Data Act /Cybersecurity

08 MAY 2023 | PRESS RELEASE

CEOs call for urgent rethink on Data Act

CEOs call for urgent rethink on Data Act before it causes lasting damage to European competitiveness and cybersecurity

Major European business leaders have written to President Von Der Leyen, Executive Vice-President Vestager, Commissioner Breton, and the Swedish Presidency, urging them to pause and rethink the Data Act. Such a monumental change to established ways of doing business without proper consideration is a huge risk both to cybersecurity and to the competitiveness of some of Europe's most successful companies.

DIGITALEUROPE and its members have three major concerns about the Data Act

1. Under the business-to-business data-sharing chapter, there are still not enough safeguards to ensure that trade secrets, cybersecurity and health and safety are secure. This represents a huge risk to the continent's competitiveness and resilience against hybrid threats, in a time of high inflation and war on our borders.

Data Act / GDPR

Brussels, 27 April 2023

Dear MEP Ms del Castillo and MEP Mr Lagodinsky, MEP Mr Bielan, MEP Mr García del Blanco, MEP Ms Kumpula-Natri, MEP Ms de la Pisa Carrión, MEP Mr Mituța, MEP Mr Boeselager, MEP Ms Lizzi, MEP Ms Kontoura,
Dear Ms Björesten and Mr Källström,
Dear Commissioner Mr Breton,

Industry representatives warn of potential conflicts between Data Act and GDPR and emphasise the importance of ensuring a fair playing field ahead of the trilogue negotiations.

We are a group of diverse stakeholders, including SMEs, representing different industries within the business community, including digital advertising and marketing. As the institutions enter trilogue negotiations on the proposal for a regulation on the harmonised rules on fair access to and use of data (the "Data Act"), we would like to reiterate our concerns about the potential unintended consequences of Article 6.2 (b). These concerns apply to the wording in the European Commission's original proposal and the Council's position that clearly interfere with the GDPR and work against achieving a level playing field and impede innovation.

DATA ACT (DA) VS. DSGVO

Prüfverfahren vor Weitergabe:

1) Sind personenbezogene Daten enthalten?
2) Handelt es sich nur um personenbezogene Daten des Nutzers?
3) Rechtfertigungsgrund gem DSGVO?

SECURITY BY DESIGN (CRA) VS. ACCESS BY DESIGN (DA)

Cyber Resilience Act (CRA)*

Annex I

1. SECURITY REQUIREMENTS RELATING TO THE PROPERTIES OF PRODUCTS WITH DIGITAL ELEMENTS

(1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks;

(2) *Products with digital elements shall be delivered without any known exploitable vulnerabilities;*

(3) *On the basis of the risk assessment referred to in Article 10(2) and where applicable, products with digital elements shall:*

a) *be delivered with a secure by default configuration, including the possibility to reset the product to its original state;*

b) *ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems*;

Data Act (DA)*

Art 3 (1) Products shall be designed and manufactured, and related services shall be provided, in such a manner that data generated by their use are, by default, easily, securely and, where relevant and appropriate, directly accessible to the user.

Art 4. (2) *The data holder shall not require the user to provide any information beyond what is necessary to verify the quality as a user pursuant to paragraph 1. The data holder shall not keep any information on the user's access to the data requested beyond what is necessary for the sound execution of the user's access request and for the security and the maintenance of the data infrastructure.*

Art 5 (3) *The user or third party shall not be required to provide any information beyond what is necessary to verify the quality as user or as third party pursuant to paragraph 1. The data holder shall not keep any information on the third party's access to the data requested beyond what is necessary for the sound execution of the third party's access request and for the security and the maintenance of the data infrastructure.*

* Jeweils basierend auf dem ursprünglichen Text des Kommissionsvorschlages

ÄNDERUNG IM RISK EXPOSURE: Verbands-Abhilfeklage wegen fehlerhaftem Produkt?

Verschuldensunabhängige Haftung (Entwurf PLD)

- Software = Produkt
- Fehlende Software-Updates unter der Kontrolle des Herstellers sowie das Versäumnis der Schwachstellenbehebung in der Cybersicherheit → Fehlerhaftes Produkt
- Cybersicherheitsschwachstellen → Fehlerhaftes Produkt (zumindest dann, wenn das Produkt verbindlichen Cybersicherheitsanforderungen nicht entspricht).
- Erweiterter "Schaden" Begriff: Verlust bzw Beschädigung von Daten, die nicht ausschließlich für berufliche Zwecke verwendet werden.

iZm Verbandsklagenrichtlinie

- Am 24.12.2020 in Kraft getreten, hätte bis 25.12.2022 in nationales Recht umgesetzt werden müssen;
- Umfassende Änderung im System der kollektiven Rechtsdurchsetzung :
- Bisher nur Möglichkeit einer Verbandsklage: Legitimierte Verbände (z.B. AK, VKI) können gesetzwidrige Bestimmungen in Musterverträgen und AGB bekämpfen und Unterlassung geltend machen.
- Neu: qualifizierte Einrichtungen sollen Verbandsklagen gegen Unternehmen erheben können, mit dem Ziel, **Unterlassung oder Abhilfe** zu erwirken (d.h. Schadenersatz, Reparatur, Ersatzleistung, Preisminderung, Vertragsauflösung oder Erstattung des gezahlten Preises)

RESÜMEE "CISO"

a) **C**ontinuous **I**nformation - up to date sein; Was kommt wann und in welchem Ausmaß (Zeitplan)?

b) **S**trategie – Inwiefern bin ich betroffen (welche Rolle nehme ich ein)? Rechte/Möglichkeiten identifizieren. Muss/will ich meine Marktstrategie, meine Produkte, meine IT-Infrastruktur anpassen? Will ich etwas "vorwegnehmen"?

c) (Interne) **O**rganisation – Wo wird die Zuständigkeit für die Umsetzungen angesiedelt? Braucht es eine eigene Digital-Compliance-Abteilung?

KONTAKT

Mag. Katharina Raabe-Stuppnig

Rechtsanwältin

T: +43 (0) 650 277 3820

E: office@raabe-stuppnig.at

KONTAKT

DR. MARIA-LUISE FELLNER

Rechtsanwältin

T: +43 (0)664 202 95 03

E: office@hands-on.legal