Hogan Lovells

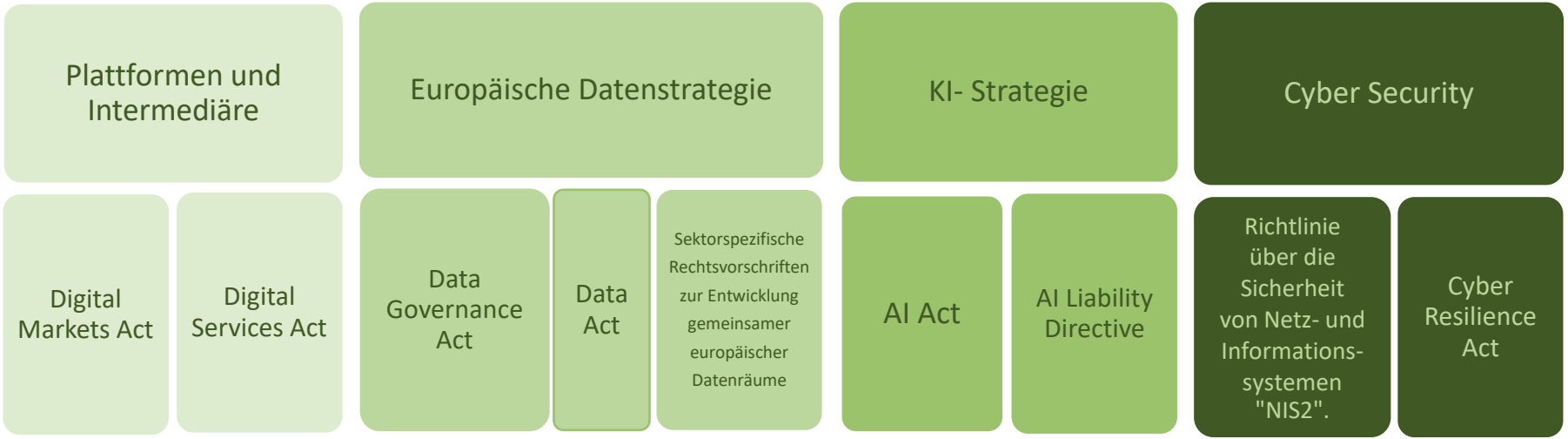
EU Digitalstrategie – Große Herausforderungen und neue Chancen für Unternehmen

24. April 2024

Sarah-Lena Kreutzmann

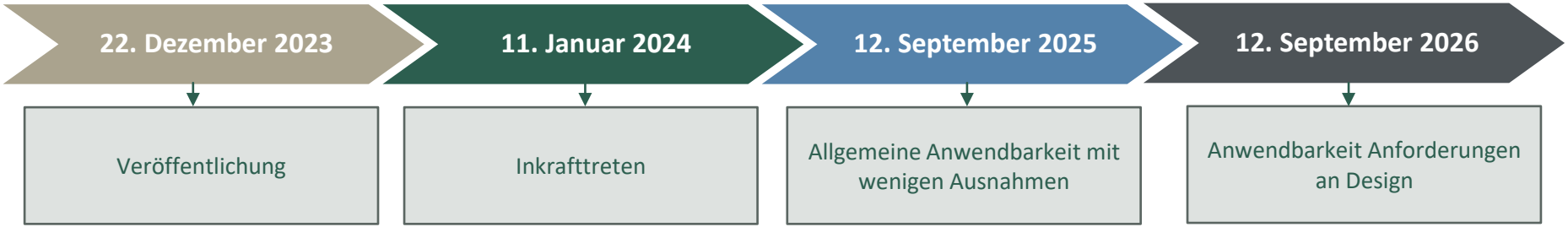
Gesetzgebung für Europas digitale Zukunft

Ausgewählte Projekte aus der EU Strategie für die Digitale Dekade



Überblick Datenverordnung

Kurzüberblick Datenverordnung



Ziel: Sektorübergreifende Verbesserung des Zugangs zu Daten, die mit digitalen Produkten oder Diensten generiert werden, unter fairen Bedingungen

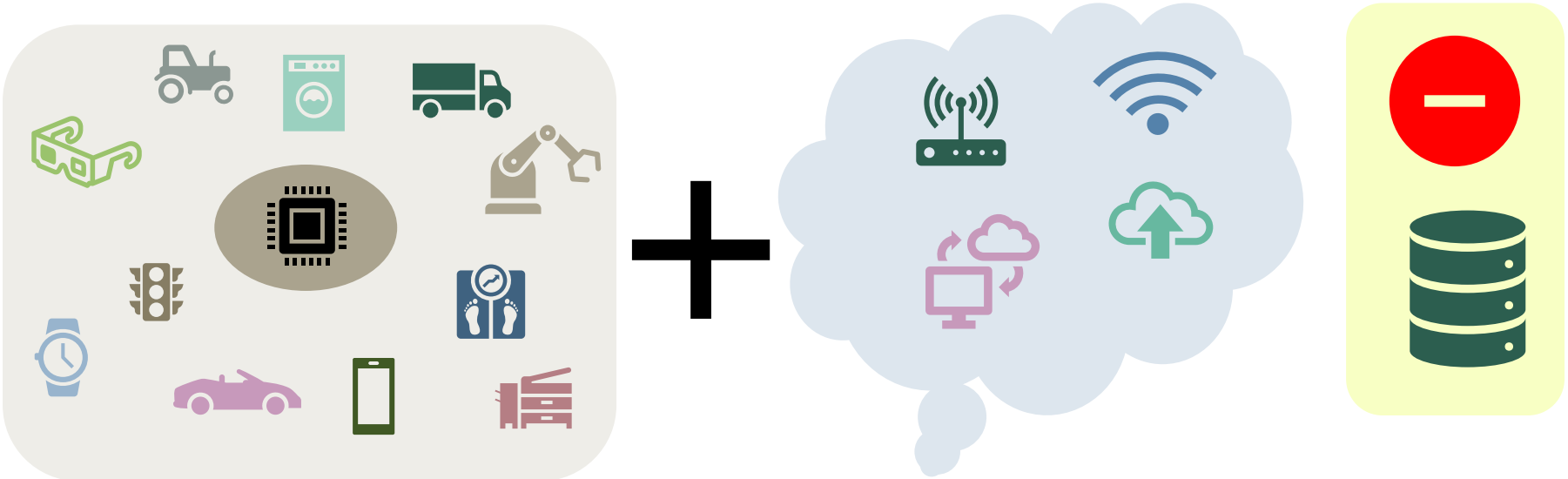
Adressaten:

- Hersteller von vernetzten Produkten und Anbieter verbundener Dienste
- Dateninhaber, Nutzer und Datenempfänger
- Geschäftsgeheimnisinhaber
- Anbieter von Datenverarbeitungsdiensten

Bußgelder: Mitgliedstaaten legen die Regeln für Sanktionen fest; teilweise Bezugnahme auf die DSGVO (bis zu EUR 20 Mio. bzw. 4 % des gesamten weltweiten Jahresumsatzes)

Was sind vernetzte Produkte?

Ein **Gegenstand,** der **Daten über seine Nutzung oder Umgebung** erlangt, generiert oder erhebt und der **Produktdaten** über einen elektronischen Kommunikationsdienst, eine physische Verbindung oder einen geräteinternen Zugang **übermitteln kann** und dessen **Hauptfunktion nicht die Speicherung, Verarbeitung oder Übertragung von Daten** im Namen einer anderen Partei – außer dem Nutzer – ist



Was sind verbundene Dienste?

Ein **digitaler Dienst** bei dem es sich nicht um einen elektronischen Kommunikationsdienst handelt, – **einschließlich Software** –, der **zum Zeitpunkt** des Kaufs, der Miete oder des Leasings **so mit dem Produkt verbunden ist**, dass das vernetzte Produkt **ohne ihn eine oder mehrere seiner Funktionen nicht ausführen** könnte oder der **anschließend** vom Hersteller oder einem Dritten **mit dem Produkt verbunden** wird, um **die Funktionen des vernetzten Produkts zu ergänzen, zu aktualisieren oder anzupassen**;

Beispiele:

- App, um die Helligkeit von Lichtern anzupassen oder die Temperatur eines Kühlschranks zu regulieren
- Anwendung für eine Waschmaschine zur Messung von Umweltauswirkungen des Waschzyklus anhand der Daten der verschiedenen Sensoren innerhalb der Maschine und Anpassung des Zyklus
- Software einer Fitnessuhr
- Bedienungs-Apps für IoT-Produkte

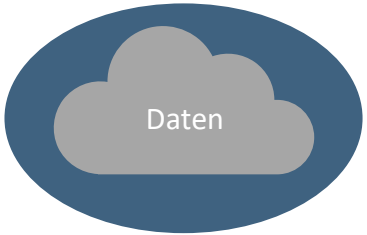
Dienste, die keine Auswirkung auf den Betrieb des vernetzten Produkts haben und keine Übertragung von Daten oder Befehlen beinhalten:

- Beratungs-, Analyse- oder Finanzdienstleistungen
- Regelmäßige Reparatur- und Wartungsdienste

Wer sind die (Haupt)Adressaten?

Dateninhaber

- Hersteller vernetzter Produkte?
- Verkäufer, Vermieter oder Leasinggeber von vernetzten Produkten?
- Anbieter verbundener Dienste?
- Inhaber von Geschäftsgeheimnissen?



Nutzer

- Eigentümer, Mieter, Leasingnehmer vernetzter Produkte
- Nutzer verbundener Dienste

Datenempfänger

- Dienstleister oder andere Vertragspartner des Nutzers (z.B. Reparatur- und Wartungsanbieter, Versicherer, Anbieter von Anschlussdienstleistungen etc.)
- Datenvermittlungsdienste
- Nicht: „Torwächter“ nach Digital Markets Act

Überblick wesentliche Herausforderungen

Zugang des Nutzers zu Produktdaten und Verbundenen Dienstdaten durch Design (**Hersteller von vernetzten Produkten / Anbieter von verbundenen Diensten**), wo dies relevant und technisch machbar ist

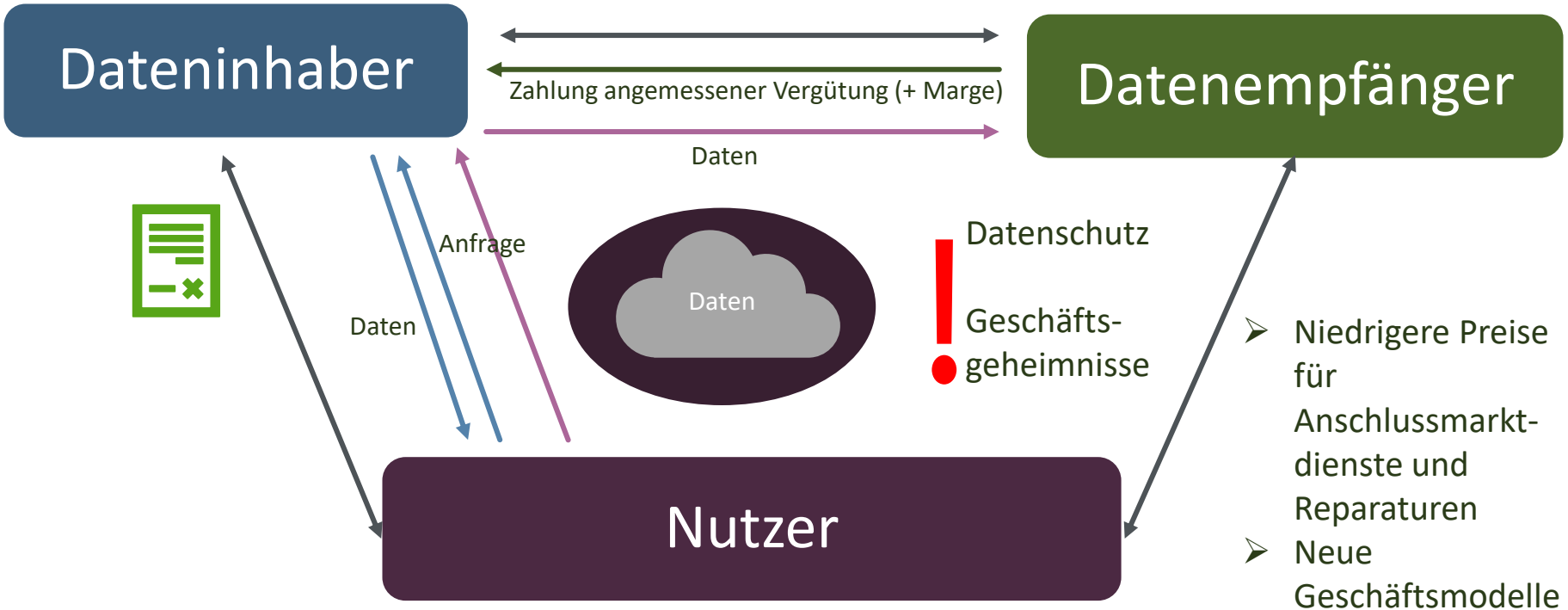
Informationspflichten gegenüber dem Nutzer (**Verkäufer, Vermieter oder Leasinggeber von vernetzten Produkten / Anbieter von verbundenen Diensten**)

Bereitstellung von ohne Weiteres verfügbaren Daten an den Nutzer auf Verlangen des Nutzers (**Dateninhaber**)

Bereitstellung von ohne Weiteres verfügbaren Daten an einen Dritten (Datenempfänger) auf Verlangen des Nutzers (**Dateninhaber**)

Vertrag mit dem Nutzer über die Nutzung von nicht-personenbezogenen ohne Weiteres verfügbaren Daten durch den Dateninhaber (**Dateninhaber**)

Bereitstellung von Daten



Regelungen für KMU

- Pflichten zur Weitergabe von Daten sind nicht anwendbar, soweit diese Daten bei Nutzung eines vernetzten Produkts oder verbundenen Dienstes generiert werden, die von einem Kleinunternehmen oder Kleinstunternehmen kommen, das
  - das kein größeres Partnerunternehmen oder verbundenes Unternehmen hat

  und
  - nicht als Unterauftragnehmer mit der Herstellung oder der Konzeption des vernetzten Produkts oder verbundenen Dienstes beauftragt wurde

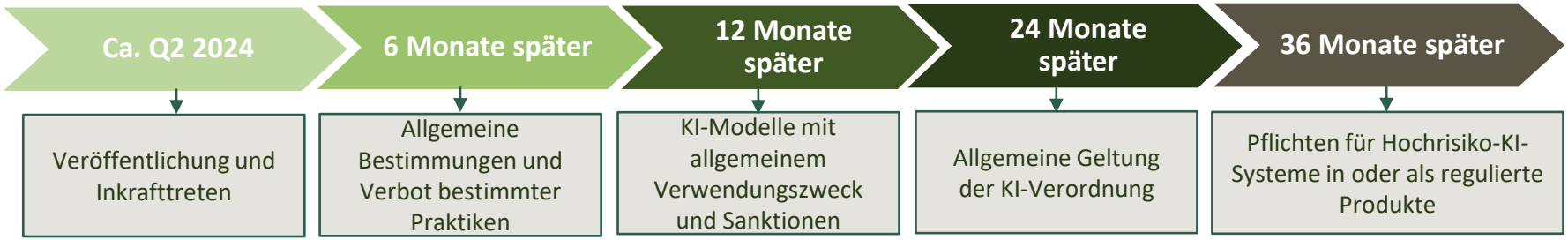
- Gegenleistung für die Weitergabe von Daten an KMU oder gemeinnützige Forschungseinrichtungen, die keine größeren Partnerunternehmen oder verbundene Unternehmen haben, darf keine Marge enthalten

Was ist jetzt zu tun?

- Prüfung der Anwendbarkeit der Datenverordnung insbesondere auf eigene Produkte und Services auf dem Markt und in Entwicklung
- Bestimmung von Art und Umfang der Daten (einschließlich personenbezogene Daten, Geschäftsgeheimnisse etc.), die generiert werden
- Berücksichtigung der Designpflichten bei Entwicklung von Produkten und Services
- Abschluss von Vereinbarungen mit Kunden zur Nutzung der Daten
- Aufbau eines Governance Programms (z.B. Bestimmung von Zuständigkeiten, Vorbereitung erforderlicher Dokumente (Informationen, AGB etc.), Schulungen etc)

Überblick KI-Verordnung

Kurzüberblick KI-Verordnung



Ziel: Schaffung eines gemeinsamen regulatorischen und rechtlichen Rahmens für vertrauenswürdige KI-Systeme mit Fokus auf Produktsicherheitsanforderungen für sogenannte Hochrisiko-KI-Systeme

Adressaten:

- Anbieter von KI-Systemen, KI-Systemen mit allgemeinem Verwendungszweck und KI-Modellen mit allgemeinem Verwendungszweck
- Einführer und Händler von KI-Systemen
- Betreiber von KI-Systemen
- Produkthersteller, die KI-Systeme zusammen mit ihrem Produkt unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringen oder in Betrieb nehmen

Bußgelder: Wirksame, verhältnismäßige und abschreckende Sanktionen mit gestaffelten Höchstbeträgen je nach Verstoß von bis zu EUR 35 / 15 / 7,5 Mio. bzw. 7 / 3 / 1 % des Umsatzes, was immer höher ist

Was sind KI-Systeme?

ein **maschinengestütztes System**, das für einen in **wechselndem Maße autonomen Betrieb** ausgelegt sind, das nach seiner Einführung anpassungsfähig sein kann und **das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet,** wie Ergebnisse wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen hervorgebracht werden, die physische oder virtuelle Umgebungen beeinflussen können

KI-System mit allgemeinem Verwendungszweck

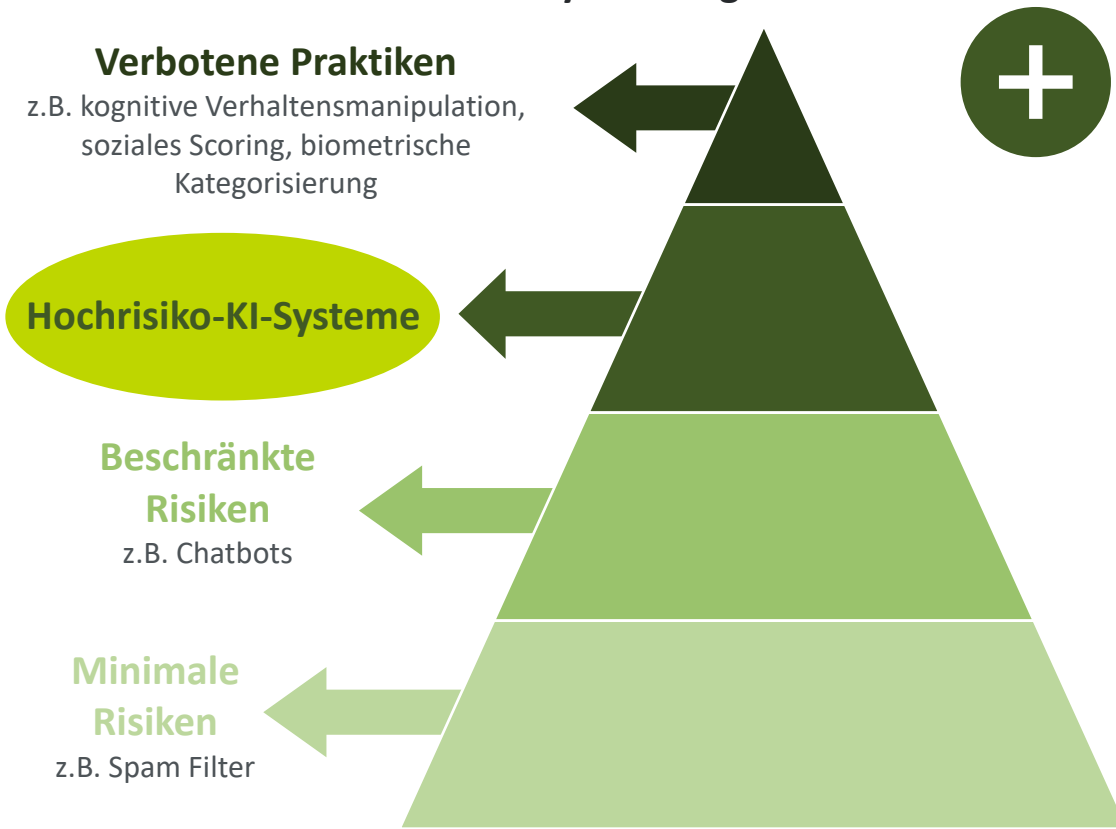
= KI-System, das auf einem **KI-Modell mit allgemeinem Verwendungszweck** beruht und in der Lage ist, **einer Vielzahl von Zwecken** sowohl für die direkte Verwendung als auch für die Integration in andere KI-Systeme zu dienen;

KI-Verordnung gilt u.a. nicht für:

- Entwicklung und Betrieb für den alleinigen Zweck der **wissenschaftlichen Forschung und Enwicklung**
- **Forschungs-, Test- und Entwicklungstätigkeiten** vor Inverkehrbringen bzw. Inbetriebnahme, jedoch **keine Tests unter realen** Bedingungen
- **Open Source KI-Systeme**, außer es handelt sich um Hochrisiko-KI-Systeme oder in bestimmten anderen Fällen (z.B. verbotene Praktiken)

Welche KI-Systeme sind betroffen?

Risko-basierter Ansatz bei KI-Systemen generell



Spezifische Regelungen für:

KI-Modelle mit allgemeinem Verwendungszweck

KI-Modelle mit allgemeinem Verwendungszweck mit systemischem Risiko

- Fähigkeiten mit hohem Wirkungsgrad
- Entscheidung der Kommission

Was sind Hochrisiko-KI-Systeme?

Bestimmte Produkte

- KI-Systeme, die
  - als **Sicherheitskomponente von Produkten** verwendet werden sollen, die bestimmten Harmonisierungsrechtsvorschriften der EU unterfallen und der **Konformitätsbewertung durch Dritte** unterliegen,

  oder

  - solche **Produkte sind**
- Beispiele:
  - Maschinen, Spielzeuge, Aufzüge, Funkanlagen, Druckgeräte, Sportbootausrüstung, Seilbahnen, Geräte zur Verbrennung gasförmiger Brennstoffe, Medizinprodukte und In-vitro-Diagnostik

Bestimmte Bereiche

- Bestimmungsgemäße Verwendung, z.B.
  - als **Sicherheitskomponenten im Rahmen der Verwaltung und des Betriebs** kritischer digitaler Infrastruktur, des Straßenverkehrs sowie der Wasser-, Gas-, Wärme- und Stromversorgung
  - für die **Einstellung oder Auswahl natürlicher Personen**,
  - für Entscheidungen, die die Bedingungen von Arbeitsverhältnissen, **Beförderungen und Kündigungen von Arbeitsvertragsverhältnissen** beeinflussen
  - für die **Kreditwürdigkeitsprüfung** und Kreditpunktebewertung natürlicher Personen

Wer sind die (Haupt)Adressaten?

Anbieter

Natürliche oder juristische Person, die ein KI-System oder ein KI-Modell mit allgemeinem Verwendungszweck

- entwickelt oder **entwickeln lässt**
- unter eigenem Namen oder Handelsmarke **in Verkehr bringt**
- unter eigenem Namen oder Handelsmarke **in Betrieb nim**mt

Einführer

Händler

Betreiber

Natürliche oder juristische Person, die

- ein KI-System **in eigener Verantwortung** verwendet,
- es sei denn, das KI-System wird im Rahmen einer **persönlichen und nicht beruflichen Tätigkeit** verwendet

Wesentliche Herausforderungen bei Hochrisiko-KI-Systemen

Pflichten des **Anbieters** beinhalten u.a.:

- Risikomanagementsystem
- Daten und Daten-Governance für Trainings-, Validierungs- und Testdatensätze
- Technische Dokumentation vor Inverkehrbringen bzw. Inbetriebnahme
- Transparenz- und Informationspflichten
- Menschliche Aufsicht
- Qualitätsmanagementsystem
- Konformitätsbewertungsverfahren
- CE-Kennzeichnung

Pflichten des **Betreibers** beinhalten u.a.:

- Maßnahmen zur Einhaltung der Gebrauchsanweisungen
- Menschliche Aufsicht durch kompetente Personen
- Überwachung des Betriebs
- Transparenzpflichten gegenüber Arbeitnehmern
- Ggf. Grundrechte-Folgenabschätzung

Was ist jetzt zu tun?

- Anwendbarkeit der KI-Verordnung prüfen, auch in Bezug auf Produkte und Services Dritter, und KI-Systeme bewerten
- Prüfung der Rolle und Pflichten in Bezug auf die KI-Systeme
- Policies im Unternehmen zum Umgang mit KI entwickeln
- Aufbau eines KI Governance Programms


Q&A

Überblick NIS2-Richtlinie und CER-Richtlinie

Kurzüberblick NIS2 und CER-Richtlinien

14. Dezember 2022	16. Januar 2023	bis Dezember 2023	18. Oktober 2024
Tag der Unterzeichnung	Inkrafttreten	Verschiedene Referentenentwürfe	Anwendung der Richtlinien durch die Mitgliedstaaten

CER-Richtlinie		NIS2-Richtlinie
KRITIS-DachG (KRITIS-Dachgesetz)		NIS2UmsuCG (Gesetz zur Umsetzung von EU NIS2 und Stärkung der Cybersicherheit)
CER: kritische Einrichtungen KRITIS-DachG: Betreiber kritischer Anlagen		NIS2: wesentliche und wichtige Einrichtungen NIS2UmsuCG: wichtige Einrichtungen, besonders wichtige Einrichtungen, Betreiber kritischer Anlagen
Resilienz und physische Sicherheit kritischer Infrastrukturen		EU-weite Mindeststandards für Cybersicherheit
Wirksame, verhältnismäßige und abschreckende Sanktionen (Höhe im KRITIS-DachG noch offen)		Wirksame, verhältnismäßige und abschreckende Sanktionen je nach Verstoß von bis zu EUR 7 [10] Mio. bzw. 1,4 [2] % des Umsatzes für [besonders] wichtige Einrichtungen (NIS2UmsuCG)

Wer ist von NIS2 bzw. NIS2UmsuCG erfasst?

Unternehmen	Sektor	Mitarbeiter*	Umsatz	Bilanz
Wesentliche / besonders wichtige Einrichtungen	NIS2 Anhang 1, NIS2UmsuCG Anlage 1 Beispiele aus Anlage 1 NIS2UmsuCG : ➢ Energieversorger, Kreditinstitute, Erbringer von Gesundheitsdienstleistungen ➢ IKT: Anbieter von Cloud-Computing Diensten, Anbieter von Rechenzentrumsdiensten, Managed Services Provider	> 250	> 50 Mio.	> 43 Mio.
Wichtige Einrichtungen	NIS2 Anhang 1 und 2, NIS2UmsuCG Anlage 1 und 2 Beispiele aus Anlage 2 NIS2UmsuCG: ➢ Hersteller von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen (u.a. Elektromotoren, Generatoren, Batterien, Kabeln, Lampen, Haushaltsgeräten) ➢ Maschinenbau (u.a. Maschinen für Metallbearbeitung, Metallerzeugung, Walzwerkseinrichtungen und Gießmaschinen) ➢ Hersteller von Kraftwagen und Kraftwagenteilen ➢ Anbieter digitaler Dienste (Online-Marktplätze, Online-Suchmaschinen, Plattform für Dienste sozialer Netzwerke)	> 50	> 10 Mio.	> 10 Mio.

Wesentliche Herausforderungen NIS2/NIS2UmsuCG

Risikomanagement:

- Generell sind geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen nach Stand der Technik zu ergreifen, um Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die für die Erbringung der Dienste genutzt werden, zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten – konkrete Mindestanforderungen (z.B. Lösungen zur Multi-Faktor-Authentifizierung)
- Ggf. Verwendung bestimmter IKT-Produkte, IKT-Dienste und IKT-Prozesse nur mit Cybersicherheitszertifizierung

Meldepflichten bei erheblichen Sicherheitsvorfällen (Erstmeldung innerhalb von 24 Stunden)

Registrierung drei Monate, nachdem ein Unternehmen erstmals oder erneut als eine besonders wichtige oder wichtige Einrichtung gilt

Pflicht zur Information der Empfänger über Sicherheitsvorfall nach Anweisung des BSI

Governance: Billigungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen

Was ist jetzt zu tun?

- Betroffenheit überprüfen (Sektor, Größe, etc.) auch anhand der lokal einschlägigen Rechtsordnungen
- Überprüfung der bereits vorhandenen Sicherheitsmaßnahmen auf etwaige Lücken
- Bestimmung und Umsetzung von ggf. erforderlichen zusätzlichen Maßnahmen, z.B. im Rahmen des Aufbaus eines umfassenden Governance Programms
- Fristgemäße Registrierung

Überblick Cyber Resilience Act

Cyber Resilience Act – Legislative Process

Ziel: Einführung gemeinsamer Cybersicherheitsvorschriften für Hersteller und Entwickler von Produkten mit digitalen Elementen (Hardware und Software), die dazu bestimmt sind, vernetzt zu werden

Adressaten:

- Hersteller von Produkten mit digitalen Elementen
- Einführer und Händler von Produkten mit digitalen Elementen

Bußgelder: Wirksame, verhältnismäßige und abschreckende Sanktionen, für bestimmte Verstöße bis zu EUR 15 Mio. bzw. 2,5 % des weltweiten Umsatzes, was immer höher ist

Was sind Produkte mit digitalen Elementen?

Ein **Software- oder Hardware-Produkt** und dessen Ferndatenverarbeitungsprozesse, einschließlich Software- oder Hardwarekomponenten, die **getrennt in Verkehr gebracht werden**

- Voraussetzung: bestimmungsgemäße oder vernünftigerweise vorhersehbare Verwendung einer direkten oder indirekten logischen oder physischen Datenverbindung zu einem Gerät oder Netz
- Open Source Software und cloud-fähige Funktionen können erfasst sein

Produkte, die heute auf dem Markt sind, können den Anforderungen unterliegen

- Medizinprodukte und In-vitro-Diagnostika
- Fahrzeuge und Systeme, Bauteile, und technische Einheiten, die unter die VO 2018/2144 fallen
- Einschränkung oder Ausschluss bei Produkten möglich, die unter andere Unionsvorschriften fallen, die sich auf alle oder einige der Risiken beziehen (z.B. Cloud Computing Dienste, die unter NIS2 fallen)
- Ersatzteile

Wesentliche Herausforderungen für Hersteller

Entwicklungsphase

- Security by design: Design, Entwicklung und Produktion auf eine Weise, dass ein angemessenes Maß an Cybersicherheit gewährleisten
- Dokumentierte Bewertung des Cybersicherheit Risikos
- Erstellung technischer Dokumentation, Gebrauchsanweisungen und anderen Informationen an Kunden

Vor Markteinführung

- Konformitätsbewertung: Selbstbewertung oder Bewertung durch Dritte
- Dokumentation: EU-Konformitätserklärung und technische Unterlagen
- Anbringung der CE-Kennzeichnung

Nach Markteinführung

- Während des Unterstützungs-zeitraums kontinuierliche Überwachung der Produktkonformität und Aktualisierung der Dokumentation
- Laufendes Schwachstellenmanagement und System zur Reaktion auf Cybervorfälle (einschließlich Meldepflichten)
- Zentrale Anlaufstelle für Nutzer

Was ist jetzt zu tun?

- Prüfung der Anwendbarkeit insbesondere auf eigene Produkte und Services auf dem Markt und in Entwicklung
- Berücksichtigung der Designpflichten bei Entwicklung von Produkten
- Konformitätsbewertungen vorbereiten
- Aufbau eines Governance Programms (z.B. Bestimmung von Zuständigkeiten, Vorbereitung erforderlicher Dokumente, Schulungen etc)


Q&A

Sarah-Lena Kreutzmann, M.A., LL.M. (Cambridge)

Counsel, Düsseldorf

Sarah-Lena Kreutzmann berät in Vertragsangelegenheiten in den Bereichen Gewerblicher Rechtsschutz und Urheberrecht, IT-Recht und Datenschutzrecht. Ihre Rechtsberatung umfasst die Beratung zu Fragen des gewerblichen Rechtsschutzes und Urheberrechts, des IT-Rechts und des Datenschutzes sowie zu kommerziellen Vertragsfragen bei Transaktionen, sowohl im Rahmen der Due Diligence als auch in Form der Beratung von Mandanten zu entsprechenden Regelungen in Kaufverträgen.

Sarah-Lena hat außerdem umfangreiche Erfahrung im Entwurf und in der Verhandlung aller Arten von technologiebezogenen Verträgen, einschließlich Outsourcing-Verträgen, Lizenz- und Übertragungsverträgen, Joint-Venture- und F&E-Verträgen sowie Verträgen über die Implementierung von IT-Systemen oder die Erbringung von IT-Dienstleistungen, unter Berücksichtigung der Anforderungen der geltenden Datenschutzgesetze.

T +49 211 1368 122

sarah-lena.kreutzmann@hoganlovells.com

Awards und Rankings

- Rising Star für Informationstechnologie und Digitalisierung, Legal 500 Deutschland, 2024

Hogan Lovells

www.hoganlovells.com