KI und Digital Law

Neues KI- und Daten-Regime im EU- Binnenmarkt

„Data Science Talk“

Es gilt das gesprochene Wort!

Bildquelle : © www.shutterstock.com agsandrew 146880227

Aus Gründen der besseren Hör- und Lesbarkeit wird teilweise oder vollständig auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche Personenbezeichnungen innerhalb der Informationen in diesem Vortrag gelten gleichwohl für beiderlei Geschlecht sowie Intersexualität.

HOCHSCHULE DER MEDIEN

Neues KI- und Daten-Regime im EU- Binnenmarkt

Gliederung

- Erwartungen/ Befürchtungen
- Chancen und Optionen der KI
- Digitale Souveränität
- **Rechtsrahmen für den Einsatz für künstliche Intelligenz**
  - KI-Verordnung/ AI-Act
  - Richtlinie über KI-Haftung (Haftung für fehlerhafte Produkte)
- **Cybersecurity**
  - NIS-2-Richtlinie zur Netzwerk- und Informationssicherheit und
  - NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG
  - Cyber Resilience Act (CRA)
- **Neues Daten-Regime im EU- Binnenmarkt für digitale Produkte und digitale Dienstleitungen**
  - Digital-Service-Act (Gesetz über digitale Dienste, DSA) und
  - Digitale Dienste-Gesetz (DDG)
  - Digital Operational Resilience Act (DORA)
  - Data-Act (DA)
- **Weitere EU-Regelwerke zum neuen digitalen Daten-Regime im EU- Binnenmarkt**
  - Digital-Markets-Act (Gesetz über digitale Märkte, DMA)
  - Data-Governance-Act (DGA)
- **Compliance & more/ Kritik**

Weiterführende Regelwerke, Strategiepapiere sowie Gutachten
Literatur
Impressum/ Disclaimer/Nutzungsbedingungen und Urheberrecht

Bildquelle© www.shutterstock.com Ase 129436517

„KI ist wahrscheinlich
das Beste
oder
das Schlimmste,
was der Menschheit passieren kann“.

Stephen Hawking, Kurze Antworten auf große Fragen, 2018

Bildquelle© www.shutterstock.com Ase 129436517

Chancen und Optionen der KI

- Insb. generative **KI** übertrifft deutlich eine Reihe kognitiver Fähigkeiten von Menschen
- Konkrete KI-Einsätze entwickeln sich schnell
- **KI-Einsätze stehen für Produktionszuwächse, Kostensenkungen, neue Geschäftsmodelle, neue Berufe, starkes Wachstum**
- Deutsches Bruttoinlandsprodukt kann bis 2030 um 220 Mrd. EUR zulegen

- **Unternehmen** benötigen KI-Strategien, lernende Strukturen, neue Kollaborationsmodelle, Effizienz und vertrauensfördernde Transparenz
- **Politik** soll wertebasierte KI-Regularien aufsetzen, ohne Innovationsfesseln anzulegen und die regulierungsbedingten Kosten im Zaum halten.
- **Bürger:** Freiheit und Wohlstand

Justenhofen, PwC Deutschland, KI, FAZ, Wirtschaftstag 2024, m.w.N.

Bei Patentanmeldungen im Bereich KI steht Deutschland weltweit auf dem 2. Platz!
F&E-Ausgaben der **DAX-Konzerne** verdoppelten sich seit 2011 auf 75 Mrd. Euro.
Konzerne wie Merck, Siemens, Apple, Google, Eli Lilly, Intel und TSMC investieren in deutsche Forschungsstandorte. Mit Unternehmen wie Aleph Alpha und **mehr als 500 KI-Start-ups kann Deutschland stark von KI profitieren.** (Quandt, FAZ, 24.06.24, S. 17.)

Technischer Fortschritt hat immer die Effekte, erstens den Wohlstand insgesamt zu vergrößern, zweitens neue Arbeitsplätze zu schaffen, drittens einige Berufe überflüssig zu machen.“
Yann LeChun, KI-Forschungschef, Facebook

Bildquelle© www.shutterstock.com Ase 129436517

HOCHSCHULE DER MEDIEN

Neues KI- und Daten-Regime im EU- Binnenmarkt

Europa will seine digitale Souveränität erhalten!

Gutachten der Datenethikkommission der Bundesregierung, Okt. 2019

„Wer von anderen übermäßig abhängig ist, wird vom „rule maker“ zum „rule taker“ und setzt seine Bürgerinnen und Bürger letztlich Vorgaben aus, die von Akteuren aus anderen Regionen der Welt formuliert werden. Bemühungen um die langfristige Sicherung der digitalen Souveränität sind daher nicht nur ein Gebot politischer Weitsicht, sondern auch Ausdruck ethischer Verantwortung.“

https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6

Personenbezogene Daten (pbD)

Information-Empires, wie Google, Meta (Amazon), Facebook, Apple

EU-Datenschutz-Grundverordnung (Gültig seit: 25. Mai 2018)

Industrie- und Unternehmensdaten

Der **Diebstahl von** IT-Geräten und **Daten sowie digitale Spionage, Wirtschaftsspionage und Sabotage** werden laut Bitkom Deutschland im Jahr 2023 rund 206 Milliarden Euro kosten. Der Schaden werde **das dritte Jahr in Folge die 200-Milliarden-Euro-Marke überschreiten**, so ein Ergebnis einer Bitkom-Umfrage unter mehr als 1.000 Unternehmen.

72 Prozent der deutschen Cybersecurity- und IT-Profis benötigen mehr Ressourcen, insb. um einen präventiven Ansatz zur Verringerung der Gefährdung ihres Unternehmens zu verfolgen.

https://www.datensicherheit.de/cyber-kriminalitaet-deutschland-2023-schaden-wert-200-milliarden-euro-erwartung, m.w.N.

Brüssel schafft einen neuen digitalen europäische Binnenmarkt!!!

Brüssel hat KI bereits wertebasiert geregelt, Rechtsrahmen für Cyber- und IT-sicherheit gestärkt und einen neuen Rechtsrahmen für den Einsatz von digitalen Dienstleistungen und digitalen Produkten in Kraft gesetzt!!!

Regelwerke z.T. bereits in Kraft, z.T. Umsetzungsfristen bis Mitte 2026!

Übersicht nicht verlieren!/ Hoher Arbeitsaufwand!

Hohe Geldbußen bis zu 40 Mio EUR oder 8% des Weltjahreshandels- eines Unternehmens

Bildquelle© www.shutterstock.com Ase 129436517

Rechtsrahmen für den Einsatz für künstliche Intelligenz

KI-Verordnung, AI-Act (Gesetz über Künstliche Intelligenz)

Künstliche Intelligenz (KI) gilt längst als Schlüsseltechnologie, die wirtschaftlich, politisch und militärisch Machtverhältnisse bestimmen wird.

Die Mitgliedstaaten der Europäischen Union haben am **02.02.24** die Verordnung zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz **(KI-Verordnung, AI-Act)** einstimmig gebilligt.
Der KI-Act wird in Deutschland zu verschiedenen Zeitpunkten in Kraft treten, je nach Art der Regelung. Die meisten Verpflichtungen des KI-Acts werden **Anfang 2026** wirksam. Regelungen für verbotene KI-Systeme treten bereits sechs Monate nach Inkrafttreten des Gesetzes in Kraft, also voraussichtlich Ende 2024. **Die Bestimmungen für allgemeine KI-Systeme werden Anfang 2025 gültig.**
(KPMG, https://kpmg.com/de/de/home/themen/2024/03/das-bedeutet-das-eu-gesetz-zur-ki.html).

Mit der KI-Verordnung gibt die EU den Rahmen für den **Einsatz von Künstlicher Intelligenz (KI)** in Europa vor. Sie will **Innovationen fördern, gleichzeitig das Vertrauen in KI stärken und sicherstellen, dass diese Technologie in einer Weise genutzt wird, die die Grundrechte und die Sicherheit der Bürgerinnen und Bürger der EU respektiert. Die KI-Verordnung stellt das weltweilt erste umfassende Regelwerk für KI dar.**
Brussels, 21.4.2021 COM(2021) 206 final
https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52021PC0206
https://www.bmj.de/SharedDocs/Pressemitteilungen/DE/2024/0202_KI-VO.html?cms_mtm_campaign=linksFromNewsletter

Für Verstöße gegen die Vorgaben der zukünftigen Verordnung sind **hohe Strafen** vorgesehen!
(bis zu 35 Mio EUR oder 7% des weltweiten Jahresumsatzes)
(Kafsack/ Armbruster, Wo die EU Künstliche Intelligenz verbieten will, FAZ, 15.04.21, S. 16.)
https://ec.europa.eu/germany/news/20210421-kuenstliche-intelligenz-eu_de
https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence
Bildquelle © www.shutterstock.com ymgerman 266978444

KI-Verordnung, AI-Act

Anwendungsbereich

Diese Verordnung gilt gem. Art. 2 der KI-Verordnung für:

a) **Anbieter,** die KI-Systeme in der Union in Verkehr bringen oder in Betrieb nehmen, unabhängig davon, ob diese Anbieter in der Union oder in einem Drittland niedergelassen sind;

b) **Nutzer** von KI-Systemen, die sich in der Union befinden;

c) **Anbieter und Nutzer** von KI-Systemen, die in einem **Drittland** niedergelassen oder ansässig sind, wenn das vom System hervorgebrachte Ergebnis **in der Union verwendet** wird.

„**System der künstlichen Intelligenz“ (KI-System):** eine Software, die mit einer oder mehreren der in **Anhang I** aufgeführten Techniken und Konzepte entwickelt worden ist und im Hinblick auf eine Reihe von Zielen, die vom Menschen festgelegt werden, Ergebnisse wie Inhalte, Vorhersagen, Empfehlungen oder Entscheidungen hervorbringen kann, die das Umfeld beeinflussen, mit dem sie interagieren (Art. 3 Abs. 1 KI-Verordnung);

ANHANG I TECHNIKEN UND KONZEPTE DER KÜNSTLICHEN INTELLIGENZ

a) Konzepte des maschinellen Lernens, mit beaufsichtigtem, unbeaufsichtigtem und bestärkendem Lernen unter Verwendung einer breiten Palette von Methoden, einschließlich des tiefen Lernens (Deep Learning);

b) Logik- und wissensgestützte Konzepte, einschließlich Wissensrepräsentation, induktiver (logischer) Programmierung, Wissensgrundlagen, Inferenz- und Deduktionsmaschinen, (symbolischer) Schlussfolgerungs- und Expertensysteme;

c) Statistische Ansätze, Bayessche Schätz-, Such- und Optimierungsmethoden.

Brussels, 21.4.2021 COM(2021) 206 final
https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52021PC0206
https://www.bmj.de/SharedDocs/Pressemitteilungen/DE/2024/0202_KI-VO.html?cms_mtm_campaign=linksFromNewsletter

HOCHSCHULE DER MEDIEN

KI-Verordnung, AI-Act

Unannehmbares Risiko

KI-Systeme, die als **klare Bedrohung für die Sicherheit, die Lebensgrundlagen und die Rechte der Menschen** gelten, sind **verboten (!!!),** Art. 5 KI-Verordnung**.**

Dazu gehören KI-Anwendungen, die den folgenden Einsatzbereich vorsehen:
Unterschwellige Techniken zur Beeinflussung des Verhaltens einer Person, die ihr oder einer dritten Person dadurch physischen oder psychischen Schaden zufügen oder zufügen können.

Ausnutzen von Schwächen einer Personengruppe aufgrund ihres Alters oder einer körperlichen oder geistigen Behinderung, um auch hier das Verhalten dieser Personen zu beeinflussen.

Einsatz von Behörden zur Bewertung oder Einstufung des sozialen Verhaltens, was nachteilige Folgen für bestimmte Personengruppen haben kann (sog. **Social Scoring**). Unter Social Scoring fallen Punktwerteverfahren, also den Versuch, soziale Phänomene oder die Eigenschaften von Personen mit Hilfe von Punktwerten zu beschreiben und damit vergleichbar zu machen.

Einsatz von **biometrischen Echtzeit-Fernidentifizierungssystemen** in öffentlich zugänglichen Räumen zum Zwecke der Strafverfolgung, sofern dies nicht für bestimmte Zwecke (z.B. Suche nach Opfern von Straftaten, Abwehr von Terroranschlägen) unbedingt erforderlich ist.

https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence

➢Bildquelle © www.shutterstock.com ymgerman 266978444

KI-Verordnung, AI-Act

Hohes Risiko (Art. 6 Abs. 2, Anhang III der KI-Verordnung)

Systeme auf Basis künstlicher Intelligenz sollen **strengen Vorgaben** unterliegen, wenn sie für die folgenden Bereiche eingesetzt werden:

1.„**Biometrische Fernidentifizierung**, ob in Echtzeit oder rückwirkend

2.Einsatz als Sicherheitskomponente in kritischen Infrastrukturen (z.B. Straßenverkehr, Wasserversorgung)

3.Schul- oder Berufsausbildung, wenn der Zugang einer Person zu einer Bildungseinrichtung beeinträchtigt werden könnte oder für die Beurteilung herangezogen wird

4.Einsatz im Personalmanagement (z.B. Einstellung, Leistungsbeurteilung, Verwaltung) sowie für den Zugang zur Selbstständigkeit

5.Zur Beurteilung für die Inanspruchnahme von wesentlichen privaten und öffentlichen Dienstleistungen (z.B. Sozialhilfeleistungen, Ermittlung der **Kreditwürdigkeit** außerhalb des Eigengebrauchs, Priorisierung von Notfalldiensten)

6. **Strafverfolgung** (z.B. Risikobewertung oder Kriminalitätsanalyse einer natürlichen Person, KI-gestützte Lügendetektoren, Bewertung der Zulässigkeit von Beweismitteln)

7.Migration, Asyl und Grenzkontrolle (z.B. Überprüfung der Echtheit von Reisedokumenten, Lügendetektoren oder Risikobewertung)

8.Rechtspflege und demokratische Prozesse (z.B. Anwendung der Rechtsvorschriften auf konkrete Sachverhalte)

All diese KI-Anwendungen können ein **hohes Risiko für die Gesundheit oder Sicherheit oder eine Beeinträchtigung der Grundrechte** mit sich führen. Neben Pflichten wie einem **Risikomanagementsystem, Qualitätsmanagement, TOMs, eine menschliche Aufsicht oder umfangreichen Transparenz- und Dokumentationspflichten, CE-Kennzeichnung)** sollen die Anbieter eine **Data Governance** aufbauen für die Trainingsdatensätze einer Künstlichen Intelligenz (Art. 10 KI-Verordnung). So werden Maßnahmen wie Pseudonymisierung, Verschlüsselung und die Beachtung des Stands der Technik gefordert.“

https://www.dr-datenschutz.de/vorschlag-eines-eu-rechtsrahmens-fuer-kuenstliche-intelligenz/
https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence
➢Bildquelle © www.shutterstock.com ymgerman 266978444

KI-Verordnung, AI-Act

Geringes Risiko: KI soll sich offenbaren (Art. 52 der KI-Verordnung)

Für KI-Systeme mit geringem Risiko für die Rechte oder Sicherheit der Bürger sollen **Transparenzvorschriften** gelten, die es ihren Nutzern ermöglichen sollen, fundierte Entscheidungen zu treffen.
So sollen insbesondere KI-Systeme, die mit Menschen interagieren (z.B. **Chatbots**) oder Inhalte generieren bzw. manipulieren (z.B. **Deep Fakes**), künftig **kenntlich machen**, dass es sich dabei um KI handelt, damit Nutzer dann bewusst entscheiden können, ob sie die Anwendung weiter nutzen wollen oder nicht.

KI mit minimalem Risiko für Rechte oder Sicherheit der Bürger von KI-Verordnung nicht erfasst

Die große Mehrheit der KI-Systeme stellt jedoch nur ein minimales oder gar kein Risiko für die Rechte oder Sicherheit der Bürger dar (z. B. **KI-gestützte Videospiele oder Spamfilter**). Diese Systeme sind von der KI-Verordnung nicht erfasst und sollen – unter Einhaltung des allgemein geltenden Rechts – weiterhin entwickelt und verwendet werden können.
Nationale Marktüberwachungsbehörden und Europäischer Ausschuss für KI sollen Verordnung durchsetzen und Verstöße sanktionieren dürfen.

Unternehmen müssen bei der Entwicklung und dem Einsatz von KI zukünftig die durch die Verordnung vorgegebenen Anforderungen berücksichtigen
Unternehmen nicht zuletzt im Hinblick auf die **hohen Sanktionsandrohungen (bis zu 35 Mio EUR oder 7% des weltweiten Jahresumsatzes)** und die fortschreitende Verbreitung von KI sind gut beraten, sich jetzt mit der Verordnung zum Einsatz von KI auseinanderzusetzen und sich mit den rechtlichen und technischen Herausforderungen des neuen Rechtsrahmens zu befassen.“ Füllsack, EU-Kommission legt weltweit ersten Rechtsrahmen für vertrauenswürdige Künstliche Intelligenz vor, https://www.cmshs-bloggt.de/tmc/eu-kommission-legt-weltweit-ersten-rechtsrahmen-fuer-vertrauenswuerdige-kuenstliche-intelligenz-vor/ 11.05.21;
Weitergehende Regelungen verpflichten die Entwickler, die Systeme im Vorfeld ausführlich auf die von Ihnen ausgehenden Risiken für die Gesundheit, die Sicherheit, die Grundrechte, die Umwelt und die Demokratie zu prüfen und im Zweifel für Abhilfe zu sorgen. Zudem müssen Entwickler sicherstellen, dass die KI-Systeme sicher sind, z.B. gegen Cyberangriffe und dokumentieren, welche Daten sie zum Training genutzt haben (Kafsack, FAZ, 15.6.23; S. 15).

KI-Verordnung, AI-Act

Vorschlag für eine Richtlinie über KI-Haftung (Haftung für fehlerhafte Produkte)

(Anpassung und Vereinheitlichung außervertraglicher zivilrechtlicher Haftung an künstliche Intelligenz), EU-Kommission, **28.09.2022**

Die Richtlinie erleichtert die Beweislast mithilfe von Offenlegung und widerlegbaren Vermutungen sehr gezielt und verhältnismäßig. Sie schafft für diejenigen, die **Schadensersatz** fordern, eine Möglichkeit, **Informationen** über Hochrisiko-KI-Systeme zu erhalten, die gemäß dem Gesetz über künstliche Intelligenz aufzuzeichnen /zu dokumentieren sind.
Verbesserter Zugang zu Beweismitteln, die sich im Besitz von Unternehmen oder Anbietern befinden.

Darüber hinaus werden diejenigen, die **Schadensersatz für durch KI-Systeme verursachte Schäden fordern**, eine angemessenere Beweislast tragen und eine Chance erhalten, mit berechtigten Haftungsansprüchen erfolgreich zu sein (Art.1) (Kausalitätsvermutung)
Fehlerquellen können sein: Mängel beim Training der KI, bei der Transparenz des Maschinenhandelns, der Möglichkeit einer Beaufsichtigung, der Datensicherheit oder einer verspäteten Fehlerkorrektur.

Die **Umsetzung der Richtlinie in nationales Recht steht noch aus** und wird erwartet, nachdem die Richtlinie das EU-Gesetzgebungsverfahren durchlaufen hat.
Nach dem derzeitigen Stand würde den Mitgliedstaaten ein Zeitraum von zwei Jahren nach Inkrafttreten der Richtlinie für die Umsetzung eingeräumt

(Brüssel, den 28.9.2022 COM(2022) 496 final)
https://single-market-economy.ec.europa.eu/document/3193da9a-cecb-44ad-9a9c-7b6b23220bcd_de
https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52022PC0496
Osborne, Clarke, https://www.osborneclarke.com/de/insights/neue-eu-richtlinie-zur-ki-haftung-was-sich-aendert-und-was-anwender-jetzt-wissen-muessen
Bildquelle © www.shutterstock.com ymgerman 266978444

Cybersecurity

NIS-2-Richtlinie –(NIS steht für Netzwerk- und Informationssicherheit)

RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES **RATES vom 14. Dezember 2022**
über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)
https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555

Allein in Deutschland werden etwa 30.000 Unternehmen von NIS 2 betroffen sein.

Geltungsbereich der neuen NIS-Richtlinie geht weit über die bisher bekannten Schlüsselunternehmen im Bereich der kritischen Infrastrukturen hinaus. Konkret wird bei NIS 2 zwischen „wesentlichen Einrichtungen“ und „wichtigen Einrichtungen“ unterschieden.

- **Wesentliche Einrichtungen** (**Essential Entities**) sind demnach Unternehmen, die in folgenden Bereichen tätig sind:
- **Energie** – Lieferung, Verteilung, Übertragung und Verkauf von Strom, Gas, Öl, Wasserstoff, Heizung sowie Ladestationen für die Elektromobilität
- **Straßen-, Schienen, Luft- und Schiffsverkehr** – dazu zählen auch Reedereien, Hafenanlagen und Flughäfen
- **Wasser** – Trink- und Abwasserversorgungsunternehmen
- **Digitale Infrastruktur und IT-Dienste** – dazu zählen auch Rechenzentren, Clouddienste, elektronische Kommunikationsdienste, Internetknoten sowie Anbieter öffentlicher elektronischer Kommunikationsnetze und -dienste
- **Bank- und Finanzwesen** – Kredit, Handel, Markt, Infrastruktur und Versicherungswesen
- **Gesundheit** – Gesundheitsdienstleister, Pharmazeutika, Hersteller medizinischer Geräte, Forschungseinrichtungen
- **Öffentliche Verwaltung** / **Raumfahrt**

- Zu den **wichtigen Einrichtungen** (**Important Entities**) werden Unternehmen folgender Bereiche gezählt:
- **Abfallwirtschaft/ Post- und Kurierdienste**
- **Chemische Erzeugnisse** – Produktion und Vertrieb
- **Lebensmittel** – Produktion und Vertrieb
- **Hersteller** – Computer, Elektronik, Optik, Maschinen, Kraftfahrzeuge und Anhänger, Transportmittel
- **Digitale Anbieter** – Suchmaschinen, soziale Netzwerke, Online-Marktplätze
- **Forschungseinrichtungen**

Bildquelle:© www.shutterstock.com Tommy Lee Walker 571378933

Cybersecurity

NIS-2-Richtlinie -

RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES **RATES vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union**, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)
https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555

Risikomanagementmaßnahmen im Bereich der Cybersicherheit (Art. 21)

- Technische, operative und organisatorische Maßnahmen
- 10 Risikomanagementmaßnahmen mit gefahrübergreifendem Ansatz

Verschärfung der Berichts- und Meldepflichten, z.B.
Unternehmen müssen ihrer nationalen Cyber Security Authority unverzüglich signifikante Störungen, Vorfälle und Cyber Threads melden. In Deutschland ist die zuständige Behörde das Bundesamt für Sicherheit in der Informationstechnik (BSI). Vorgesehen ist dafür ein dreistufiger Prozess:

- **Innerhalb von 24 Stunden muss direkt nach Bekanntwerden eines Vorfalls ein vorläufiger Bericht übermittelt werden.**
- **Innerhalb von 72 Stunden** muss ein vollständiger Bericht folgen, der auch eine erste Bewertung des Vorfalls enthält.
- **Innerhalb eines Monats** muss ein Abschlussbericht eingereicht werden, der detaillierte Beschreibungen des Vorfalls, der Art der Bedrohung und der grenzüberschreitenden Auswirkungen enthält.

Verschärfung der Sanktionsmaßnahmen

Außer der Meldepflicht für Vorfälle verschärft NIS 2 auch die Sanktionen für die Missachtung der Vorgaben.
Bei wesentlichen Einrichtungen können die Bußgelder bis zu 10 Millionen EUR oder 2 Prozent des weltweiten Jahresumsatzes betragen, je nachdem welcher Betrag höher ist.
Bei wichtigen Einrichtungen ist das maximale Bußgeld auf 7 Millionen EUR oder 1,4 Prozent des weltweiten Jahresumsatzes gedeckelt.

Bildquelle:© www.shutterstock.com Tommy Lee Walker 571378933

Cybersecurity

NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG

Die EU-Mitgliedsstaaten müssen NIS 2 bis zum **17. Oktober 2024** in nationales Recht umsetzen.

Referentenentwurf des Bundesministeriums des Innern und für Heimat
Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG)
https://intrapol.org/wp-content/uploads/2023/07/230703_BMI_RefE_NIS2UmsuCG.pdf

Welche Unternehmen die NIS-2-Vorgaben erfüllen müssen, richtet sich nach der Unternehmensgröße und dem Umsatz (§ 28 E-NIS2UmsuCG).

Besonders wichtige Einrichtung

a) mindestens 250 Mitarbeiter beschäftigt, **oder**

b) einen Jahresumsatz von über 50 Millionen Euro und zudem eine Jahresbilanzsumme von über 43 Millionen Euro aufweist;

Eine wichtige Einrichtung

a) mindestens 50 Mitarbeiter beschäftigt **oder**

b) einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro aufweist;

Bildquelle:© www.shutterstock.com Tommy Lee Walker 571378933

Der Referentenentwurf des Bundesinnenministeriums sieht insb. vor, dass **Geschäftsführer und andere Leitungsorgane** von Unternehmen für die Einhaltung der Risikomanagementmaßnahmen **mit ihrem Privatvermögen haften**.

D&O- sowie Cyberversicherung!

Bildquelle:© www.shutterstock.com Tommy Lee Walker 571378933

Cybersecurity

NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG

Die EU-Mitgliedsstaaten müssen NIS 2 bis zum **17. Oktober 2024** in nationales Recht umsetzen.

Beispiel Risikomanagementmaßnahmen (§ 30 E-NIS2UmsuCG)
Betroffene Einrichtungen und Unternehmen müssen verhältnismäßige **technische und organisatorische Maßnahmen** zum Schutz ergreifen. Diese Maßnahmen sollen auf einem **gefahrenübergreifenden Ansatz** beruhen. Dabei müssen Maßnahmen mindestens folgende Bereiche betreffen:

- Risikoanalyse und Sicherheit für Informationssysteme
- Bewältigung von Sicherheitsvorfällen
- Aufrechterhaltung des Betriebes, wie Backup-Management, Wiederherstellung nach einem Notfall und Krisenmanagement
- **Sicherheit der Lieferkette** (s.a. Richtlinie EU 2022/2464 Nachhaltigkeitsberichterstattung von Unternehmen)
- Sicherheit bei Erwerb, Entwicklung und Wartung von IT-Systemen, Komponenten und Prozessen, einschl. Management und Offenlegung von Schwachstellen
- Konzepte und Verfahren zur Bewertung von Risikomanagementmaßnahmen im Bereich Cybersicherheit
- Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit
- Kryptografie und Verschlüsselung
- Sicherheit des Personals und Konzepte für die Zugriffskontrolle und Management von Anlagen
- Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierliche Authentifizierung
- Gesicherte Sprach-, Video- und Textkommunikation
- Sichere (Notfall-)Kommunikationsysteme

Darüber hinaus sind besonders wichtige Einrichtungen und wichtige Einrichtungen sowie Domain-Name-Registry-Diensteanbieter verpflichtet, sich spätestens nach 3 Monaten beim BSI selbst zu registrieren und ihre Daten zu übermitteln (§ 32)

Bildquelle:© www.shutterstock.com Tommy Lee Walker 571378933

Cybersecurity

Cyber Resilience Act (EU-Gesetz über Cyberresilienz), ergänzt den NIS2 Rahmen

Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020, Brüssel, den 15.9.2022 COM(2022) 454 final 2022/0272(COD)

Inkrafttreten: Die Verordnung soll in 2024 in Kraft treten. Die Hersteller müssen die Vorschriften 24 Monate nach ihrem vor. Inkrafttreten anwenden: **Mitte 2025** (Art. 66 i.V.m. Art. 11 Meldepflichten der Hersteller) und **generell Mitte 2026.**

Von Babymonitoren bis hin zu Smartwatches, **Produkte und Software, die eine digitale Komponente enthalten,** sind in unserem täglichen Leben allgegenwärtig. Weniger offensichtlich für viele Benutzer ist das Sicherheitsrisiko, das solche Produkte und Software darstellen können.

Mit dieser Verordnung wird Folgendes festgelegt (Art. 1):

a) Vorschriften für das **Inverkehrbringen von Produkten mit digitalen Elementen, um die Cybersicherheit solcher Produkte zu gewährleisten;**

b) grundlegende **Anforderungen an die Konzeption, Entwicklung und Herstellung von Produkten mit digitalen Elementen sowie Pflichten der Wirtschaftsakteure in Bezug auf diese Produkte hinsichtlich der Cybersicherheit;**

c) grundlegende Anforderungen an die von den Herstellern festgelegten Verfahren zur **Behandlung von Schwachstellen, um die Cybersicherheit von Produkten mit digitalen Elementen während ihres gesamten Lebenszyklus zu gewährleisten**, sowie **Pflichten der Wirtschaftsakteure in Bezug auf diese Verfahren**;

d) Vorschriften für die **Marktüberwachung** und die Durchsetzung der oben genannten Vorschriften und Anforderungen.

Diese Verordnung gilt für Produkte mit digitalen Elementen, deren bestimmungsgemäße oder vernünftigerweise vorhersehbare Verwendung eine direkte oder indirekte logische oder physische Datenverbindung mit einem Gerät oder Netz einschließt.

https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52022PC0454

Sie gilt für alle Produkte, die direkt oder indirekt mit einem anderen Gerät oder Netzwerk verbunden sind, mit Ausnahme bestimmter Ausschlüsse wie Open-Source-Software oder Dienste, die bereits unter bestehende Vorschriften fallen, was für Medizinprodukte, Luftfahrt und Autos der Fall ist.

https://digital-strategy.ec.europa.eu/de/policies/cyber-resilience-act

Bildquelle:© www.shutterstock.com Tommy Lee Walker 571378933

Cybersecurity

Cyber Resilience Act (CRA) (EU-Gesetz über Cyberresilienz), ergänzt den NIS2 Rahmen

Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020, Brüssel, den 15.9.2022 COM(2022) 454 final 2022/0272(COD)

Grundlegende Anforderungen an Cybersicherheitsniveau, wie z.B.: Authentifizierungs-, Identitäts- oder Zugangsverwaltungssysteme, Vertraulichkeit und Verschlüsselung personenbezogener oder sonstiger Daten, durch modernste Mechanismen, Integrität, Datenminimierung, Abwehrfähigkeit gegen Überlastungsangriffe auf Server (Denial-of-Service-Angriffe), etc.

Maßnahmen:
Bewertung der Cybersicherheitsrisiken, technische Dokumentation, Sorgfaltspflichten, Risikobewertung, Schwachstellenbehandlung, Konformitätsbewertungsverfahren, EU-Konformitätserklärung, Aufbewahrungspflichten, Cybersicherheitszertifizierung, Informations- und Anleitungspflichten, Korrekturmaßnahmen, Meldepflichten, Marktüberwachungsbehörden, etc.

Sanktionen
Geldbußen von bis zu 15 000 000 EUR oder – im Falle von Unternehmen – von bis zu 2,5 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt, je nachdem, welcher Betrag höher ist.

Die Verordnung soll 2024 in Kraft treten. Die Hersteller müssen die Vorschriften 36 Monate nach ihrem Inkrafttreten anwenden. Die Kommission wird das Gesetz dann regelmäßig überprüfen und über dessen Funktionsweise berichten.

Bildquelle:© www.shutterstock.com Tommy Lee Walker 571378933

Neues Daten-Regime für digitale Produkte und digitale Dienstleitungen

Digital-Service-Act (Gesetz über digitale Dienste, DSA)

Verordnung (EU) 2022/2065 vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste) https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022R2065

Inkrafttreten: 17.02.2024 (Artikel 24 Absätze 2, 3 und 6, Artikel 33 Absätze 3 bis 6, Artikel 37 Absatz 7, Artikel 40 Absatz 13 und Kapitel IV Abschnitte 4, 5, und 6 gelten jedoch ab dem 16. November 2022.

Es wurde die Grundlage geschaffen, besser gegen Hassrede, Markenpiraterie oder unsichere Produkte vorzugehen.

Anwendungsbereich

Alle Online-Vermittler, die ihre Dienste im Binnenmarkt anbieten, müssen die neuen Vorschriften beachten.
Online-Anbieter sind zum Beispiel Internetanbieter, Domänennamen-Registrierstellen, Hosting-Dienste wie Cloud- und Webhosting-Dienste, Online-Marktplätze, App-Stores, Plattformen der kollaborativen Wirtschaft und Social-Media-Plattformen.
Mit der Verordnung werden **Pflichten und ein System der Verantwortung und Transparenz von Anbietern von Vermittlungsdiensten** eingeführt,

Für sehr große Online-Plattformen und Suchmaschinen gelten besondere Regularien, weil diese besondere Risiken für die Verbreitung illegaler Inhalte und für Schäden in der Gesellschaft bergen.
Für große Online-Plattformen und Suchmaschinen, die monatlich mindestens 45 Millionen aktive Nutzerinnen und Nutzer erreichen, gelten besondere Sorgfaltsanforderungen, wie zum Beispiel die Pflicht zur Risikoanalyse und Risikominimierung.
https://www.bundesregierung.de/breg-de/themen/digitalisierung/gesetz-ueber-digitale-dienste-2140944
https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022R2065

Zudem hat der Deutsche Bundestag das Digitale-Dienste-Gesetz (DDG) beschlossen.
Es regelt nationale Details zum Digital Services Act (DSA) der EU. Im Zentrum des Regelwerks: Welche Behörden sind in Deutschland wofür zuständig?
Inkrafttreten: 14.05.2024
Das Digitale Dienste Gesetz (DDG) ist nicht nur für große Online-Plattformen und Tech-Giganten relevant, sondern auch für **kleine und mittelständische Unternehmen (KMU), die digitale Dienste anbieten**.
Das DGG gilt für alle Dienstanbieter – Anbieter digitaler Dienste (§ 1 Abs. 1)

Bildquelle © www.shutterstock.com ymgerman 266978447

Neues Daten-Regime für digitale Produkte und digitale Dienstleitungen

Digital Operational Resilience Act (DORA)

Digitale operationale Resilienz im Finanzsektor, Anwendbar ab dem 17.01.2025

VERORDNUNG (EU) 2022/2554 DES EUROPÄISCHEN PARLAMENTS UND DES RATES
vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011, Amtsblatt der Europäischen Union, 27.12.2022 L 333/1
https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R2554

Der Digital Operational Resilience Act (DORA) schafft einen verbindlichen, umfassenden Rahmen für das Risikomanagement im Bereich der Informations- und Kommunikationstechnologie (IKT) für den EU-Finanzsektor als auch ihre Finanzdienstleister
https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022R2554

Anforderungen Art. 1
(Auswahl)
Risikomanagement im Bereich der Informations- und Kommunikationstechnologie (IKT);
Verschiedene Meldepflichten
Tests der digitalen operationalen Resilienz;
Maßnahmen für das solide Management des IKT-Drittparteienrisikos;
Anforderungen in Bezug auf vertragliche Vereinbarungen zwischen IKT-Drittdienstleistern und Finanzunternehmen
……

https://www.haufe.de/compliance/recht-politik/eu-digital-operational-resilience-act-dora_230132_571156.html

Es besteht die Befürchtung, dass die spezifischen, technischen Regelungen nicht für alle Unternehmen gleichermaßen geeignet sind. In der Praxis zeigt sich eine erhebliche Komplexität bei den notwendigen Vertragsverhandlungen mit den IKT-Dienstleistern. **Der DORA stellt sowohl Finanzunternehmen als auch ihre Dienstleister vor Aufgabenstellungen, die oft nur von großen Unternehmen mit eigenen Governance-Abteilungen bewältigt werden können**.
KMUs fallen oft aus dem Raster.
(Wulf, FAZ, IT-Sicherheit wird zur Mammutaufgabe, 24.04.24, S. 16)

Bildquelle © www.shutterstock.com ymgerman 266978447

Neues Daten-Regime für digitale Produkte und digitale Dienstleitungen

Data-Act

Verordnung 2023/2854 über harmonisierte Vorschriften **für einen fairen Datenzugang und eine faire Datennutzung“ (kurz: Data Act) Anwendbar ab dem 12.09.2025**
https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202302854

Mit der zunehmenden digitalen Vernetzung von Haushalten, Fahrzeugen und Industrie wächst das Datenvolumen rasant. Mit diesem **Datenpotential l**assen sich **neue Geschäftsmodelle oder Dienstleistungen** entwickeln. **Jedoch werden 80% bis 95% der Industrie- und Unternehmensdaten nicht genutzt.** Viele Hersteller gewähren keinen oder bestenfalls beschränkten Zugriff auf die gesammelten Daten, klagen Zulieferer über die Autokonzerne, Handwerksverbände über Heizungshersteller oder wie die Lufthansa über Airbus.

Ziel ist es, durch mehr Datennutzung **zu mehr Wertschöpfung,** insbesondere für **neue Geschäftsmodelle, Start-Ups und KMUs**, beizutragen.
Insbesondere enthält der Data Act Vorschriften hinsichtlich

- „der **Datenweitergabe von Unternehmen an Verbraucher (B2C) und zwischen Unternehmen (B2B),**
- der **Pflichten der Dateninhaber**, die nach dem Recht der EU verpflichtet sind, **Daten bereitzustellen** (inkl. **Entgeltregelungen im B2B-Bereich**),
- des **Verbots missbräuchlicher Vertragsklauseln** für den Datenzugang und die Datennutzung zwischen Unternehmen (B2B),
- der **Bereitstellung von Daten für öffentliche Stellen** wegen außergewöhnlicher Notwendigkeit (B2G) sowie
- vertraglicher Regelungen und der technischen Umsetzung beim Wechsel zwischen Datenverarbeitungsdiensten („**Cloud Switching**“)“.

https://bmdv.bund.de/DE/Themen/Digitales/Digitale-Gesellschaft/EU-Data-Act/eu-data-act.html
https://bmdv.bund.de/SharedDocs/DE/Anlage/DG/Digitales/eu-data-act-deutsche-fassung-22-12-23.pdf?__blob=publicationFile

Personenbezogene Daten sind durch den Data-Act im Prinzip nicht betroffen (ErwG 7)

Artikel 41 Mustervertragsklauseln und Standardvertragsklauseln

Verband Deutscher Maschinen- und Anlagenbau (VDMA):

„Ein massiver Eingriff in die gut funktionierende Vertragsfreiheit im Datenaustausch zwischen den Unternehmen“

Zentralverband des deutschen Handwerks (ZDH):

“die Kunden hätten nun die Entscheidungsfreiheit, an wen sie ihre Daten weitergeben und zu welchem Zweck“

(Kafsak, Brüssel hebt den Datenschatz, FAZ, 29.06.23, m.w.N. S. 18)

Bildquelle © www.shutterstock.com ymgerman 266978447

Weitere EU-Regelwerke zum neuen digitalen Daten-Regime

Digital-Markets-Act (Gesetz über digitale Märkte, DMA), Anwendbar seit 2.05.2023

VERORDNUNG (EU) 2022/1925 vom 14.09.2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte)

https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022R1925

„Auf den digitalen Märkten fungieren einige **große Online-Plattformen** als **„Gatekeeper**“.

Das Gesetz über digitale Märkte stellt sicher, dass es auf diesen Plattformen fair zugeht. Gemeinsam mit dem Gesetz über digitale Dienste ist es eines der Kernelemente der EU-Digitalstrategie.

Die Gatekeeper-Kriterien sind erfüllt, wenn ein Unternehmen

- eine starke wirtschaftliche Position mit erheblichen Auswirkungen auf den Binnenmarkt innehat und in mehreren EU-Ländern aktiv ist,
- über eine starke Vermittlungsposition verfügt, d. h. eine große Nutzerbasis mit einer großen Anzahl von Unternehmen verbindet,
- eine gefestigte und dauerhafte Position auf dem Markt hat (oder bald haben wird). Als über längere Zeit stabil gelten Unternehmen, wenn sie die beiden vorgenannten Kriterien in jedem der letzten drei Geschäftsjahre erfüllt haben.

Vorteile

- Gewerbliche Nutzer, die auf Gatekeeper angewiesen sind, um ihre Dienstleistungen im Binnenmarkt anzubieten, können sich auf ein freuen.
- **Für Innovatoren und Technologie-Sfaireres Geschäftsumfeld start-ups bieten sich neue Möglichkeiten, im Umfeld von Online-Plattformen zu konkurrieren und innovativ zu sein, ohne sich an unfaire Bedingungen halten zu müssen, die ihre Entwicklung bremsen.**
- Verbraucher/innen können mehr und bessere Dienstleistungen wählen und eher ihren Anbieter wechseln, haben direkten Zugang zu Dienstleistungen und fairen Preisen.
- Den Gatekeepern bleiben alle Möglichkeiten, innovativ zu sein und neue Dienstleistungen anzubieten**. Sie dürfen nur gegenüber den von ihnen abhängigen gewerblichen Nutzern und Kunden keine unlauteren Praktiken anwenden, um einen unbilligen Vorteil zu erlangen.“**

https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_de

Bildquelle © www.shutterstock.com ymgerman 266978447

Weitere EU-Regelwerke zum neuen digitalen Daten-Regime

Data-Governance-Act, wirksam ab 24.09.2023

Verordnung (EU) 2022/868 des Europäischen Parlaments und des Rates vom 30.05.2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt)
https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32022R0868

…. bietet einen Rahmen, um das Vertrauen in den **freiwilligen Datenaustausch zum Nutzen von Unternehmen und Bürgern** zu stärken.

„Der öffentliche Sektor verfügt über große Mengen geschützter Daten (z. B. **personenbezogene Daten und vertrauliche Geschäftsdaten)**, die nicht als offene Daten wiederverwendet werden können, aber nach spezifischen EU- oder nationalen Rechtsvorschriften wiederverwendet werden könnten. **Aus diesen Daten kann eine Fülle von Wissen gewonnen werden, ohne dass deren geschützte Natur beeinträchtigt wird, und die DGA sieht Regeln und Garantien vor, um eine solche Weiterverwendung zu erleichtern, wann immer dies nach anderen Rechtsvorschriften möglich ist.“**

„DGA stellt ein sektorübergreifendes Instrument dar, das darauf abzielt,

- die **Weiterverwendung von öffentlich/gespeicherten, geschützten Daten** zu **regulieren**,
- die gemeinsame Nutzung von Daten durch die Regulierung **neuartiger Datenvermittler** und die gemeinsame Nutzung von **Daten für altruistische Zwecke** zu fördern.
- Sowohl personenbezogene als auch nicht personenbezogene Daten befinden sich im Anwendungsbereich der DGA, und wenn es um personenbezogene Daten geht, gilt die **Datenschutz-Grundverordnung (DSGVO).**
- Zusätzlich zur DSGVO werden **integrierte Sicherheitsvorkehrungen** das Vertrauen in den Datenaustausch und die Weiterverwendung stärken, was eine Voraussetzung für die Bereitstellung von mehr Daten auf dem Markt ist.“

Beispiel**: „Die Deutsche Telekom** bietet mit ihrem **Data Intelligence Hub** einen Datenmarkt, auf dem Unternehmen Informationen von hoher Qualität, z. B. Produktionsdaten, sicher verwalten, bereitstellen und monetarisieren können, um Prozesse oder ganze Wertschöpfungsketten zu optimieren. Die Telekom übernimmt die Rolle eines neutralen Treuhänders und garantiert Datenhoheit durch dezentrales Datenmanagement. Derzeit sind mehr als 1.000 Nutzer aus über 100 verschiedenen Unternehmen auf der Plattform aktiv.
https://digital-strategy.ec.europa.eu/de/policies/data-governance-act-explained

Bildquelle © www.shutterstock.com ymgerman 266978447

Compliance & more

- **Gesellschaftliche, technische und organisatorische Herausforderungen**
- **Konformität mit den neuen digitalen Daten-Regime erreichen (Compliance)!!!**
- **Frühzeitige Befassung/ Übergangsfristen nutzen!!!**
- **Zukunftssichernde Investitionen!!!**
  Rechtssichere Umsetzung, Infrastruktur und Technologieauswahl,
  interdisziplinäres Expertenteam, Auswahl, Aus- Fort- und Weiterbildung der Mitarbeiter
- Transferbeschleunigung/ **Geschäftsmodelle** entwickeln
- Allianzen schmieden!
- KI- sowie Cyber-Versicherung!
- **Zukünftigen Wohlstand gerecht verteilen!!!**

Vorteile nutzbar machen, Nachteile minimieren und uns ethisch verantwortungsbewusst verhalt

- **Lebenslanges Lernen!**

(„Tamdiu discendum est, quamdiu nescias. Man muss so lange lernen, wie man (etwas) nicht weiß“. **Seneca** in: Epistulae morales 76,3 fährt fort, wenn man einem antiken Sprichwort Glauben schenke, müsse man sogar so lange lernen, wie man lebe.)

KRITIK

- Start-ups, KMUs werden mit großen Unternehmen und den zu bewältigenden hochkomplexen Aufgaben wieder einmal in einen Topf geworfen (Proportionalität?!)
  (z.B.: Androhung hoher Bußgelder, gleiche Übergangsvorschriften)
- Übereifer des Gesetzgebers?! Mehrere gesetzgeberische Großvorhaben gleichzeitig und eigentlich wie abgestimmt?!
- Regulierungen sollten nicht gegen Unternehmer sowie Konsumenten arbeiten und sie auch nicht überfordern!
- Wenn Unternehmen aufgeben oder ins Ausland abwandern oder in die Insolvenz gehen, hat die Regulierung ihr Ziel verfehlt!
- Mehr Führungskräfte sollten nach politischer Verantwortung streben!
- Dachgesellschaften wie **Berufekammern, Verbände, IHKs**, etc.???
  (Modelle zur Umsetzung von Gesetzen/ Standards, Code of Conducts, etc., damit sich nicht zehntausende KMUs individuell mit den neuen Vorgaben beschäftigen müssen – Beispiel Art. 40 DSGVO!!!)

Bildquelle © www.shutterstock.com ymgerman 266978447

Weiterführende Regelwerke, Strategiepapiere sowie Gutachten

- Europäisches Parlament: Bericht mit Empfehlungen a.d. Kommission zu zivilrechtlichen Regelungen im Bereich Robotik (2015/2103(INL), 2017
- EUROPÄISCHE KOMMISSION, GENERALDIREKTION KOMMUNIKATIONSNETZE, INHALTE UND TECHNOLOGIEN, ETHIK-LEITLINIEN FÜR EINE VERTRAUENSWÜRDIGE KI, PUBLICATIONS OFFICE, 2019, https://DATA.EUROPA.EU/DOI/10.2759/22710
- Europäisches Parlament: Entwurf eines Berichtes mit Empfehlungen an die Kommission zu zivilrechtlicher Haftung beim Einsatz künstlicher Intelligenz vom 27.04.2020, 2020/2014(INL): 7
- Entschließung des Europäischen Parlaments mit Empfehlungen an die Kommission zu dem Rahmen für die ethischen Aspekte von künstlicher Intelligenz, Robotik und damit zusammenhängenden Technologien, 2020
- Europäische Kommission: Weißbuch zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen. COM 2020; 65 final
- Europäische Kommission: Verordnungsentwurf für einen Rechtsrahmen für den Einsatz für künstliche Intelligenz in sensiblen Feldern (Brussels, 21.4.2021 COM(2021) 205 final)
- Entwurf für eine Richtlinie über KI-Haftung, Brüssel, den 28.9.2022 COM(2022) 495
- Dt. Ethikrat, Stellungnahme Mensch und Maschine – Herausforderungen durch Künstliche Intelligenz, 2023
- Gutachten der Datenethikkommission der Bundesregierung zum Schutz der Gesellschaft vor den Folgen übergriffiger KI, 2019
- Strategie Künstliche Intelligenz der Bundesregierung, 2018
- Strategie Künstliche Intelligenz der Bundesregierung - Fortschreibung 2020
- Datenstrategie der Bundesregierung, 2021
- Sachverständigenrat: Digitalisierung für Gesundheit – Ziele und Rahmenbedingungen eines dynamisch lernenden Gesundheitssystems" SVR-Gutachten, 2021
- Weitere Regelwerke, etc. auf den Folien und beim Referenten

Bildquelle © www.shutterstock.com ymgerman 266978447

Literatur

- Armbruster, (Hrsg.): Künstliche Intelligenz für Jedermann, 2018, m.w.N.
- Beck: Über Sinn und Unsinn von Statusfragen – zu Vor- und Nachteilen der Einführung einer elektronischen Person, in: Hilgendorf/Günther (Hrsg.): Robotik und Gesetzgebung. Beiträge der Tagung vom 7. bis 9. Mai 2012 in Bielefeld, Baden-Baden, 2013, S. 255 ff.
- Bendel: 300 Keywords Informationsethik. Grundwissen aus Computer-, Netz- und Neue-Medien-Ethik sowie Maschinenethik, 2016.
- Bundesregierung, Eckpunkte der Bundesregierung für eine Strategie Künstliche Intelligenz, 18.07.2018, https://www.bmwi.de/Redaktion/DE/Downloads/E/eckpunktepapier-ki.pdf?__blob=publicationFile&v=8.
- Eberl: Smarte Maschinen. Wie Künstliche Intelligenz unser Leben verändert, 2016.
- Europäisches Parlament, Bericht mit Empfehlungen a.d. Kommission zu zivilrechtlichen Regelungen im Bereich Robotik (2015/2103(INL), 2017; ENTWURF EINER ENTSCHLIESSUNG DES EUROPÄISCHEN PARLAMENTS mit Empfehlungen an die Kommission zu zivilrechtlichen Regelungen im Bereich Robotik (2015/2103(INL),
- Fachforum Autonome Systeme im Hightech-Forum: Autonome Systeme. Chancen und Risiken für Wirtschaft, Wissenschaft und Gesellschaft, 2016.
- Ford: Aufstieg der Roboter. Wie unsere Arbeitswelt gerade auf den Kopf gestellt wird – und wie wir darauf reagieren müssen, 2016, S. 38 f.
- Finlay: Artificial Intelligence and Machine Learning for Business: A No-nonsense Guide to Data Driven Technologies-Artificial Intelligence and Machine Learning, 2018, S. 1 ff.
- Fioranelli: Künstliche Intelligenz, Robotik sowie autonome Systeme in der Pflege aus ethischer, gesundheitsökonomischer und rechtlicher Sicht, 2017, m.w.N.
- Görz/Schneeberger/Schmid: Handbuch der künstlichen Intelligenz, 2014.
- Hanisch: Zivilrechtliche Haftungskonzepte für Robotik, in: Hilgendorf (Hrsg.): Robotik im Kontext von Recht und Moral, 2014.

Bildquelle© : Klein-www.eldorado-design.de/Eldorado/Agentur.html

Literatur

- Hanika: ChatGPT & Co. in der Zahnmedizin – Ein Muss für die zukunftssicherer Praxis! (Teil II), KN Kieferorthopädie Nachrichten, Juni 2024, S. 1, 18-20.
- Hanika: ChatGPT & Co. in der Zahnmedizin – Ein Muss für die zukunftssicherer Praxis! (Teil I), KN Kieferorthopädie Nachrichten, Mai 2024, S. 1, 18-20.
- Hanika: Die Zukunft des Menschen – Künstliche Intelligenz, Robotik und autonome Systeme in der Gesundheitsversorgung, in: Hanika (Bandhrsg.), Künstliche Intelligenz, Robotik und autonome Systeme in der Gesundheitsversorgung, Schriften zu Gesundheitsökonomie/ Gesundheitsmanagement , hrsg. von Erbsland/ Häusler, Tagungsband 2019.
- **Hanika: Digitalisierung und Big Data im Universum des Rechts - Zur guten digitalen Ordnung am Beispiel der Gesundheitswirtschaft, 2. Aufl. 2021, S. 268 ff.**
- Hanika: Künstliche Intelligenz, Robotik und autonome Systeme in der Pflege, PflegeRecht, 2018.
- Hoeren: Rechtsgutachten zum Umgang mit KI-Software im Hochschulgesetz, in: Salden/ Leschke: Didaktische und rechtliche Perspektiven auf KI-gestütztes Schreiben in der Hochschulbildung, 2023.
- John: Haftung für künstliche Intelligenz. Rechtliche Beurteilung des Einsatzes intelligenter Softwareagenten im E-Commerce, 2007.
- Jorzig: Wer haftet bei KI im Gesundheitswesen?, Management & Krankenhaus 6/21, S. 15.
- Knoll/Christaller: Robotik, 2003 / Kreutzer/Sirrenberg: Künstliche Intelligenz verstehen, 2019.
- Ministerium für Schule und Bildung des Landes Nordrhein-Westfalen, Umgang mit textgenerierenden KI-Systemen – Ein Handlungsleitfaden, 02/2023.
- Neuhäuser: Roboter und moralische Verantwortung, in: Hilgendorf, (Hrsg.): Robotik im Kontext von Recht und Moral, 2014.
- Ross: Die Wirtschaftswelt der Zukunft. Wie Fortschritt unser komplettes Leben umkrempeln wird, 2016.
- Schweighöfer: Vorüberlegungen zur elektronischen Person, in: Schweighofer/Menzel/ Kreuzbauer (Hrsg.): Auf dem Weg zur ePerson, Wien, 2001, S. 45 ff.
- Zaiser, Generative AI, 3.9.2022.
- Weitere Literatur auf den Folien und beim Referenten

Bildquelle© : Klein-www.eldorado-design.de/Eldorado/Agentur.html

Impressum/ Disclaimer/Nutzungsbedingungen und Urheberrecht

Referent
Prof. Dr. iur. Heinrich Hanika
Prinz-Rupprecht-Str. 24
67146 Deidesheim
Germany

Kontakt
Tel.: +49 (0) 6326 982445
Fax.: +49 (0) 6326 982446
Email: heinrich@h-hanika.de

Dieser Vortrag stellt eine allgemeine unverbindliche Information dar. Die Inhalte spiegeln die Auffassung von Prof. Dr. Hanika im Zeitpunkt des Vortrags wider.

KI und Digital Law – das neue KI- und Daten-Regime im EU- Binnenmarkt unterliegen einem raschen und fortwährenden Wandel, so dass alle Ausführungen immer nur dem Wissensstand zum Zeitpunkt der Ausführungen entsprechen können.

Obwohl die Informationen mit großer Sorgfalt erstellt wurden, besteht kein Anspruch auf und keinerlei Gewähr für sachliche Richtigkeit, Vollständigkeit, Korrektheit, Qualität und/ oder Aktualität. Insbesondere kann dieser Vortrag nicht den besonderen Umständen des Einzelfalles Rechnung tragen. Eine Verwendung liegt daher in der eigenen Verantwortung des Nutzers.

Bitte beachten Sie, dass die rechtlichen Informationen keine Rechtsauskunft bzw. Rechtsberatung dar. In rechtlichen oder steuerrechtlichen Zweifelsfällen erteilen Rechtsanwälte und Steuerberater entsprechende Auskünfte.

Haftungsansprüche gegen den Referenten und/ oder den Veranstalter, die sich auf Schäden materieller oder immaterieller Art beziehen, welche durch die Nutzung oder Nichtnutzung der dargebotenen Informationen bzw. durch die Nutzung fehlerhafter oder unvollständiger Informationen verursacht wurden, sind grundsätzlich ausgeschlossen.

Der Referent freut sich auf Anregungen, Hinweise und Verbesserungsvorschläge, die dann ggf. zukünftig Berücksichtigung finden können. Es wird empfohlen, den vorliegenden Vortrag **im Einzelfall auf den jeweiligen Stand der Rechtsentwicklung** hin zu überprüfen.

Dem Nutzer wird grundsätzlich empfohlen ggf. **Rücksprache** mit zuständigen Aufsichtsbehörden, Bundesverbänden, **Kammern,** Gesellschaften, Landesdatenschutzbeauftragten, weiteren Rechtskundigen, Steuerberatern, **Cyber- und Haftpflichtversicherungen** sowie spezialisierten Experten, Ministerien und Behörden zu nehmen und im jeweiligen Einzelfall die Nutzung von Digitalisierungsmaßnahmen, Datenschutz- und Datensicherheitsrecht , Big Data sowie Big Data Strategien abzuklären.

Nutzungsbedingungen und Urheberrecht

Texte, Bilder, Grafiken sowie die Gestaltung dieser Seiten unterliegen dem Urheberrecht. Sie dürfen -unter Beachtung der Zitierregeln- die Texte ausschließlich für Zwecke des Studiums, für Erwerbszwecke sowie Zwecke ihres Arbeitgebers verwenden. Weiterhin unterliegen Bilder sowie ggf. Texte und sonstige Dateien ganz oder teilweise dem Urheberrecht Dritter. Auch über das Bestehen von Rechten Dritter gibt Ihnen der für den Inhalt verantwortliche Referent nähere Auskünfte. Sofern Ihnen in diesen Fällen die Urheber nicht ersichtlich sein sollten, können Sie diese bei dem Referenten erfragen.

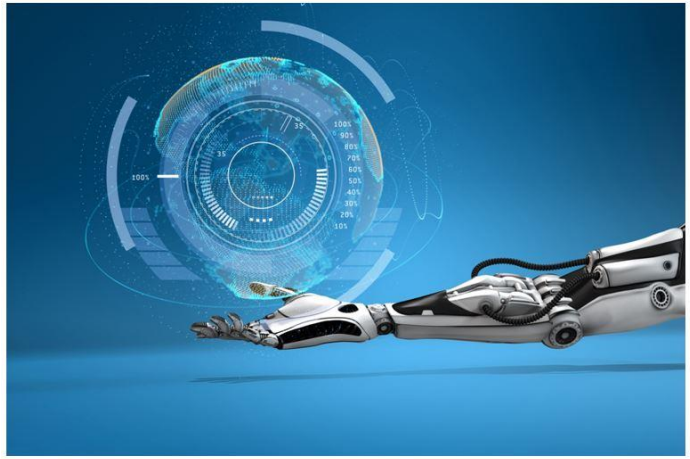
Eine Vervielfältigung oder Verwendung dieser Seiten oder Teilen davon in anderen elektronischen oder gedruckten Publikationen und deren Veröffentlichung ist nur mit unserer Einwilligung gestattet. Diese erteilt auf Anfrage der für den Inhalt verantwortliche Referent.

HOCHSCHULE DER MEDIEN

Herzlichen Dank

für Ihr

geschätztes Interesse !



Bildquelle:© www.shutterstock.com Willyam Bradberry 265382450

Nutzungsrechte an Photos: H. Hanika; Bilder, die mit Lizenzen von Shutterstock.com, Klein-www.eldorado-design.de/Eldorado/Agentur.html, Zitt verwendet werden:

- Bildquelle S. 1**:** © www.shutterstock.com agsandrew 146880227
- Bildquelle S. 2 - 5: © www.shutterstock.com Ase 129436517
- Bildquelle S. 6 - 11: © www.shutterstock.com ymgerman 266978444
- Bildquelle S. 12 - 17: © www.shutterstock.com Tommy Lee Walker 571378933
- Bildquelle S. 18 -25: © www.shutterstock.com ymgerman 266978447
- Bildquelle S. 26 und 27: © : Klein-www.eldorado-design.de/Eldorado/Agentur.html
- Bildquelle S. 29: shutterstock.com Willyam Bradberry 265382450