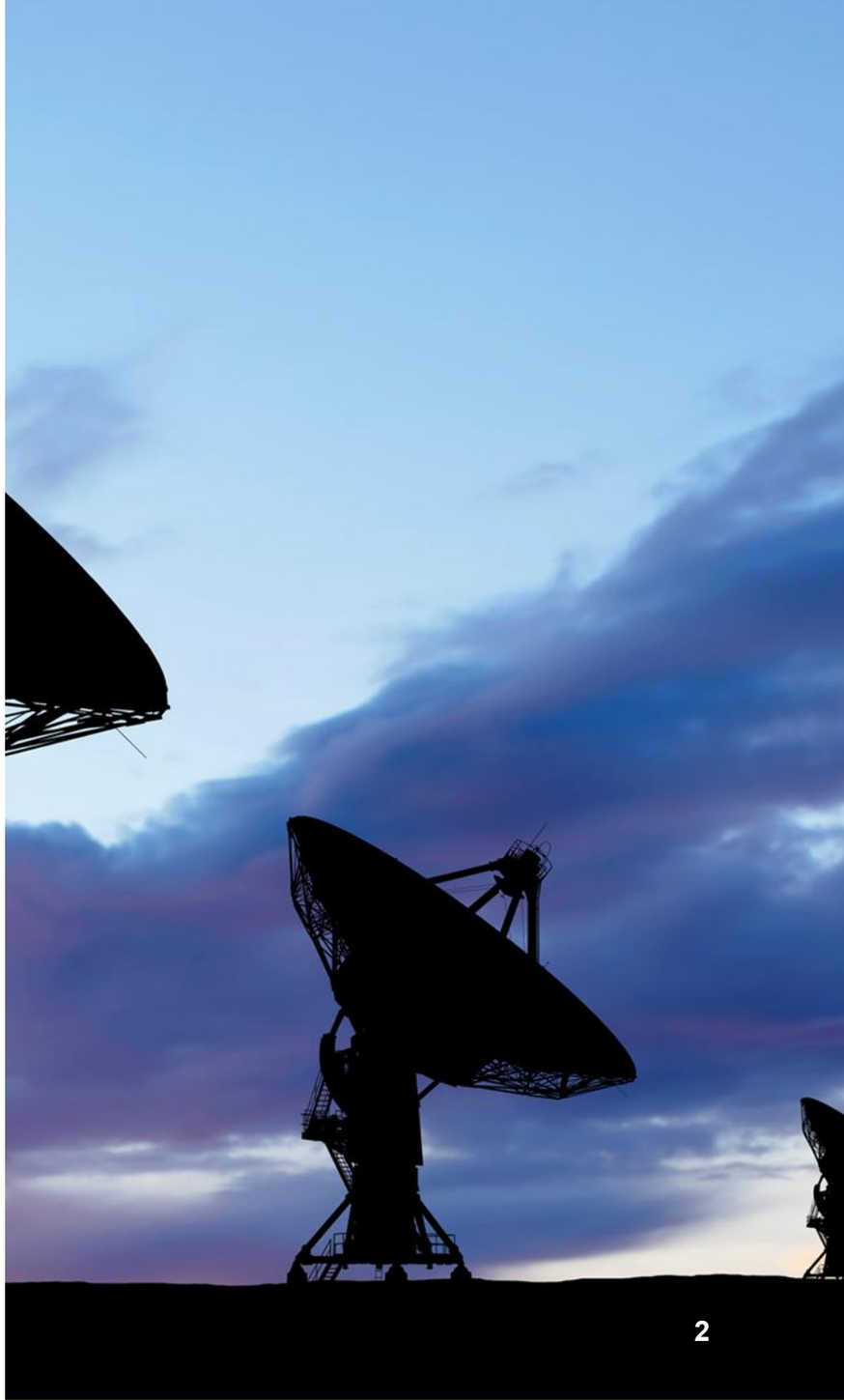
TaylorWessing

Die neuen EU-Digitalgesetze

Follow the sun Webinar I Taylor Wessing

2. September 2025 I Dr. Axel Frhr. von dem Bussche

Überblick



1 | Europäische Digitalstrategie

TaylorWessing

Überblick über die EU-Gesetz-gebung im digitalen Sektor

Stand: 21. August 2025

Research & Innovation	Industrial Policy	Connectivity	Data & Privacy	IPR	Cybersecurity	Law Enforcement	Trust & Safety	E-commerce & Consumer Protection	Competition	Finance
Digital Europe Programme Regulation	Recovery and Rexilience Facility Regulation	Frequency Bands Directive	…	Database Directive	Regulation for a Cybersecurity Act	Law Enforcement Directive	Toys Regulation	…	EU Merger Regulation	Common VAT system
Horizon Europe Regulation	InvestEU Programme Regulation	Radio Spectrum Decision	**GDPR**	Community Design Directive	European Cybersecurity Centre	Directive: combating fraud	European Standardization Regulation	**EU accessibility Act (EEA)**	Technology Transfer	Administrative cooperation (Tax)
Regulation on a pilot regime distributed ledger tech. Market	Connecting Europe Facility Regulation	Broadband Cost Reduction Directive	Regulation on the free flow of non-personal data	Enforce-ment Directive	**NIS-2-Directive**	Interoperability between EU information systems in the field of borders and visa	eIDAS Regulation	Geo-Blocking Regulation	Company Law Directive	Payment Service Directive 2
	Regulation on Joint Undertakings under Horizon Europe	Open Internet Access Regulation	Open Data Directive	Directive on the protection of trade secrets	Information Security Regulation	Regulation on terrorist content online	Radio Equipment Directive	Regulation on cooperation for the enforcement of consumer protections laws	Market Surveillance Regulation	**Digital Operational Resilience Act (DORA)**
	Decision on a path to the Digital Decade	EECC	**Data Governance Act (DGA)**	Design Directive	Cybersecurity Regulation	Temporary CSAM Regulation	Regulation for a Single Digital Gateway	Digital content Directive	P2B Regulation	Crypto-assests Regulation (MiCAR)
	European Chips Act	EU-top-level-domain Regulation	**Data Act (DA)**	Compulsory licensing of patents	**Cyber Resilience Act (CRA)**	E-evidence Regulation	General Product Safety Regulation	Directive on certain aspects concerning for the sale of goods	Single Market Programme	Financial Data Access Regulation
	European critical raw materials Act	Roaming Regulation	European Health Data Space	Standard essential patents	Cyber Solidarity Act	Directive on combating violence against women	Machinery Regulation	**Digital Services Act (DSA)**	Vertical Block Exemption Regulation	Payment Services Regulation
	Net Zero Industry Act	Secure Connectivity Programme Regulation	Data collection for short-term rental Regulation			Digitalization of travel documents	**AI Act**	Political Advertising Regulation	**Digital Markets Act (DMA)**	Digital euro
	STEP	RSPP 2.0	Interoperable Europe Act				**(New) Product Liability Directive**	Rights to repair Directive	Regulation on distortive foreign subsidies	Regulation on combating late payment
	EU Space Law	Digital Networks Act	ePrivacy Regulation				**AI Liability Directive**	e-invoicing Directive	Platform Work Directive	EU-Business Wallet
	European supercomputer capacity to AI-start-ups		**Digital Networks Act**					Multimodal digital mobility services	Single Market Emergency Instrument	

Applicable law	Published in the Official Journal of the EU
In negotiation	Proposal by the Commission entered the legislative process
Planed initiative	Mentioned by the Commission as potential legislative initiative
Abandoned	Negotiations failed

2 | Umgang mit KI und EU KI-VO

TaylorWessing

KI-VO – Im Überblick

Gegenstand

• Weltweit erste KI-Regulierung zur Regulierung von KI-Systemen und KI-Modellen mit allgemeinem Verwendungszweck (GPAI-models)

•„Produkt-Compliance“, Marktüberwachung und –kontrolle
→ **KI-VO = Produktsicherheitsrecht**

Ziel der KI-VO

• Sicherheit der EU-Bürger

• Grundrechtsschutz

• Vertrauen und Akzeptanz für KI als Technologie

• Förderung von Innovation

Wer ist betroffen?

- Anbieter von KI-Systemen oder Modellen
- Betreiber von KI-Systemen
- Produkthersteller, die KI-Systeme zusammen mit ihrem Produkt in Verkehr bringen
- Extraterritorialer Ansatz

Sanktionen?

- Bis zu EUR 35 Millionen oder bis zu 7 % des weltweiten Umsatzes
- Verwaltungsrechtliche Maßnahmen (auch das Verbot KI-Systeme anzubieten)

KI-VO: Timeline

- Regelungen gelten bereits

21. April 2021

- EU Kommission: Vorschlag

2. February 2025

- **KI-Kompetenz** des Personals
- **Verbotene KI-Praktiken**

2. August 2025

- KI-Modelle mit allgemeinem Verwendungszweck (**GPAI**)
- Aufsichtsbehörden, Governance und Sanktionen

2. August 2027

- **Eingebettete Hochrisiko-KI** (**Art. 6 Abs.** iVm. Anhang I)
- GPAI, die vor dem 2. August 2025 in Verkehr gebracht wurde

12. July 2024

- Veröffentlichung im Amtsblatt

2. May 2025 (at the latest)

- **Praxisleitfäden** sind verfügbar, Art. 56 Abs. 9

2. August 2026

- **Allgemeine Anwendbarkeit der KI-VO**

Insbesondere:

- **Transparenzanforderungen**
- **Nicht eingebettete Hochrisiko-KI (Art. 6 Abs. 2** iVm. Anhang III)

2. August 2030

- Hochrisiko-KI, die bestimmungsgemäß von Behörden genutzt werden und vor dem 2. August 2026 in Verkehr gebracht wurden

31. December 2030

- KI-Systeme, die Komponenten von **IT-Großsystemen** sind (Annex X) und die vor dem 2. August 2027 in Verkehr gebracht oder in Betrieb genommen wurden.

KI-Systeme, die vor dem Geltungsbeginn der KI-VO in Verkehr gebracht oder in Betrieb genommen wurden, unterfallen der KI-VO nur, soweit sie *wesentlich* verändert wurden. Art 111 KI-VO

Persönlicher und räumlicher Anwendungsbereich der KI-VO

Persönlich und **Räumlich**: Regelungsadressaten finden sich in Art. 2 Abs. 1 KI-VO

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

b) **Betreiber** von KI-Systemen, die ihren **Sitz in der Union** haben oder **in** der **Union befinden**;

c) **Anbieter** und **Betreiber** von KI-Systemen, die ihren **Sitz in einem Drittland** haben oder **sich in einem Drittland befinden**, **wenn** die vom KI-System **hervorgebrachte Ausgabe in der Union verwertet wird**

d) **Einführer** und **Händler** von KI-Systemen:

e) **Produkthersteller**, die KI-Systeme zusammen mit ihrem Produkt unter ihrem eigenen Namen oder ihrer Handelsmarke [**in der Union**]* in Verkehr bringen oder in Betrieb nehmen

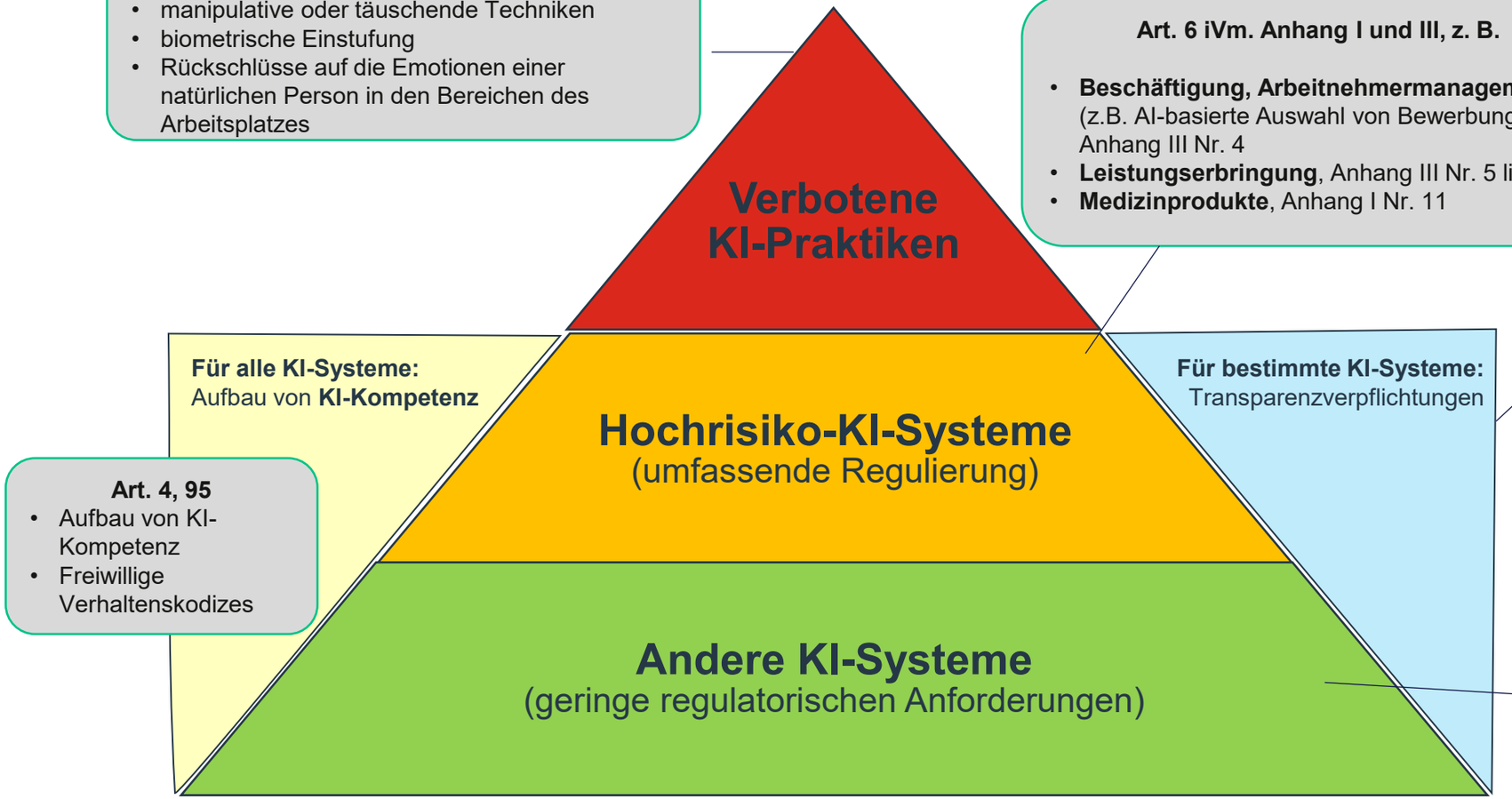
f) **Bevollmächtigte von Anbietern**, die **nicht in der Union niedergelassen** sind

g) **Betroffene Personen**, die sich **in der Union** befinden

*vgl. Art. 1 Abs. 2 lit. a, Art. 25 Abs. 3 KI-VO

Risikobasierter Ansatz der KI-VO !

Art. 5 (1), z.B.
- manipulative oder täuschende Techniken
- biometrische Einstufung
- Rückschlüsse auf die Emotionen einer natürlichen Person in den Bereichen des Arbeitsplatzes



Art. 6 iVm. Anhang I und III, z. B.
- **Beschäftigung, Arbeitnehmermanagement** (z.B. AI-basierte Auswahl von Bewerbungen), Anhang III Nr. 4
- **Leistungserbringung**, Anhang III Nr. 5 lit. a
- **Medizinprodukte**, Anhang I Nr. 11

Art. 50, z.B.
- die für die direkte Interaktion mit natürlichen Personen bestimmt sind (z. B. Chatbots)
- Erzeugung von synthetischen Audio-, Bild-, Video- oder Textinhalten (insbesondere GPAI)
- Erstellung oder Manipulation von Texten, die mit dem Ziel der Information der Öffentlichkeit veröffentlicht werden

Art. 4, 95
- Aufbau von KI-Kompetenz
- Freiwillige Verhaltenskodizes

Leitfaden der Kommission, C(2025) 924 final:
"Die überwiegende Mehrheit der Systeme, selbst wenn sie als KI-Systeme im Sinne von Artikel 3 Nr. 1 KI-VO eingestuft werden, unterliegen nicht den regulatorischen Anforderungen KI-VO."

nur Art. 4, 95 KI-VO

Risikoeinstufung

Hochrisiko-KI
(umfassende Regulierung)

Hochrisiko-KI:

Eingebettete KI

Art. 6 Abs. 1 + Anhang I

Sicherheitsbauteil eines Produkts oder das Produkt selbst
+
Unterliegt einer Konformitätsbewertung

Geräte, die gasförmige Brennstoffe verbrennen

Zivilluftfahrt

Sportboote

Spielzeug

Medizinische Geräte

Landwirtschaftliche Fahrzeuge

Nicht eingebettete KI

Art. 6 Abs. 2 + Anhang III

Allgemeine und berufliche Bildung

Arbeit: Beförderungs-/Entlassungsentscheidungen

Leistungserbringung

Rekrutierung

Versorgung mit Energie

In Abweichung von Art. 6 (2) **gelten** die in Anhang III genannten KI-Systeme **nicht als hochriskant, wenn beabsichtigt ist:**

Art. 6 Abs. 3 UAbs.1

- eine enge verfahrenstechnische Aufgabe zu erfüllen;
- das Ergebnis einer bereits abgeschlossenen menschlichen Tätigkeit zu verbessern;
- Entscheidungsmuster oder -abweichungen zu erkennen und es nicht dazu gedacht ist, die zuvor durchgeführte menschliche Bewertung zu ersetzen oder zu beeinflussen, ohne dass eine ordnungsgemäße menschliche Überprüfung stattfindet;
- eine vorbereitende Aufgabe für eine Bewertung durchzuführen

Art. 6 Abs. 3 UAbs. 2

und es kein Profiling von natürlichen Personen durchführt

Anforderungen der KI-VO: Kurzüberblick

„Normale“ GPAI-Modelle:

- Technische Dokumentation
- Compliance mit Urheberrechten
- Detaillierte Zusammenfassung
- Verhaltenskodex

GPAI-Modelle mit systemischem Risiko

- Modellbewertung & Belastungstests
- Systemisches Risikoassessment & Cybersicherheitsmaßnahmen
- Melden schwerwiegender Vorfälle & Energieeffizienzberichte

Hochrisiko-KI-Systeme:

- Dokumentation
- Qualität
- Transparenz
- Risikomanagement
- Menschliche Überwachung
- Cybersicherheitsmaßnahmen
- Folgenabschätzung für Grundrechte
- Konformitätsbewertungsverfahren

3 | Europäische Datenstrategie (Data Act und Data Governance Act)

Data Governance Act (DGA)

Gegenstand

- Schaffung einer Infrastruktur für (freiwilligen) Datenaustausch
- Abbau technischer Hürden

Ziel des DGA

Datenverfügbarkeit herstellen, Vertrauen in Datenaustausch stärken, Überwindung technischer Hürden

→**Digitale Transformation** (durch weitreichende Datenzugriffe und Verwendungsmöglichkeiten)

→**Bessere Bewältigung von gesellschaftlichen Herausforderungen** (z.B. Klimawandel, Mobilitätswende)

Wer ist betroffen?

- Öffentliche Stellen
- Anbieter von Datenvermittlungsdiensten

Wann?

Trat am 23. Juni 2022 in Kraft;
seit dem **24. September 2023** vollumfassend anwendbar

DGA: Maßnahmen

Datenverfügbarkeit

- **Weiterverwendung bestimmter Kategorien im Besitz öffentlicher Stellen** (z.B. geheime statistische Daten des Statistischen Bundesamts, an dem eine Forschungseinrichtung Interesse hat)
- **Datenvermittlungsdienste als Schlüsselrolle in der Datenwirtschaft** (z.B. durch Datenmarktplätze für Datenaustausch zw. Unternehmen)
- **Datenaltruismus – Anreize für Datenspenden**

Stärkung des Vertrauens in Datenaustausch

- **Vermeidung von Interessenskonflikten**
- **Unabhängigkeit der Preisgestaltung**
- **Strukturelle Trennung**
- **Transparenz, Fairness & Compliance**
- **Diskriminierungsfreier Zugang**

Abbau technischer Hürden

- **Anforderungen an Neutralität und Interoperabilität**
- **Angemessenes Schutzniveau**

Data Act (DA)

Gegenstand

Förderung der Verfügbarkeit und Nutzbarkeit von Daten (personenbezogene und nicht personenbezogene Daten) in der EU durch:

- Datenzugangs- und Datennutzungsansprüche
- Interoperabilität von Daten und erleichtertem Wechsel zwischen Datenverarbeitungsdiensten (insb. Cloud)
- Verpflichtung Daten unter außergewöhnlichen Umständen offenzulegen (B2G)

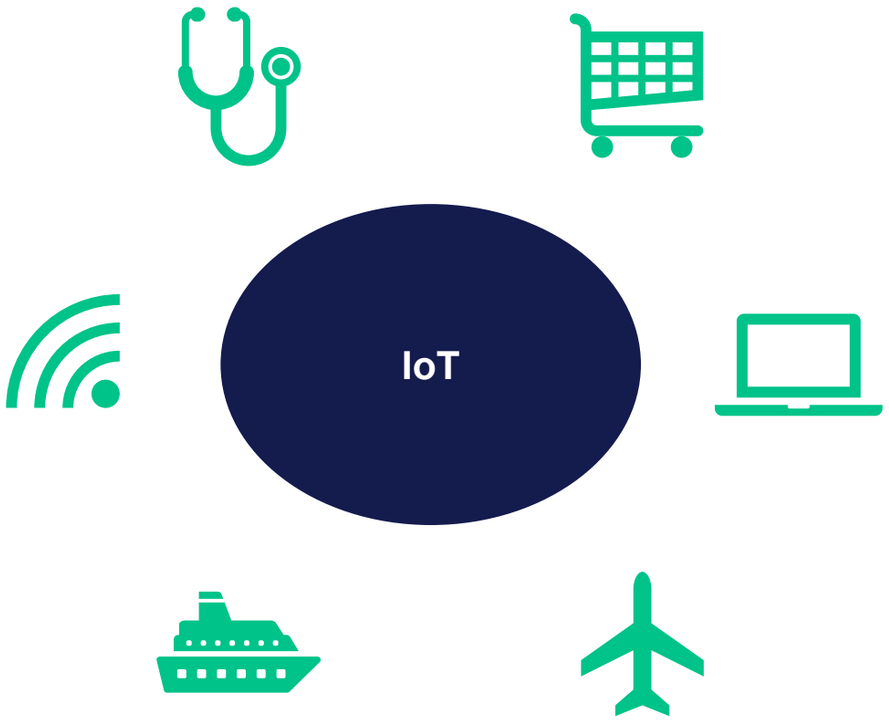
Wer ist betroffen?

- Dateninhaber
- Hersteller von vernetzten Produkten oder verbundenen Diensten
- Nutzer
- Datenempfänger / Dritte
- Datenverarbeitungsdienste

Wann?

Trat am 11. Januar 2024 in Kraft; wird ab dem **12. September 2025** weitestgehend anwendbar

Sachlicher Anwendungsbereich
Datenzugang: Vernetzte Produkte



ISO/IEC 30141:2024 (Referenzarchitektur)

Wesentliche Eigenschaften von vernetzten / IoT-Produkten, Art. 2 Nr. 5 DA:

- Körperlicher Gegenstand
- **Datenerhebung:** Produkt erhebt durch seine Komponenten oder sein Betriebssystem Daten über seine Leistung, Nutzung oder Umgebung („**Produktdaten**“, Art. 2 Nr. 15 DA).
- **Datenübermittlung:** Produkt übermittelt die Produktdaten über einen elektronischen Kommunikationsdienst, eine physische Verbindung oder einen geräteinternen Zugang (z.B. terrestrische Telefonnetze, Fernsehkabelnetze, Satellitennetze und Nahfeldkommunikationsnetze).

- **Entscheidend:** Inverkehrbringen auf dem Unionsmarkt
- **Ausgeschlossen:** Prototypen

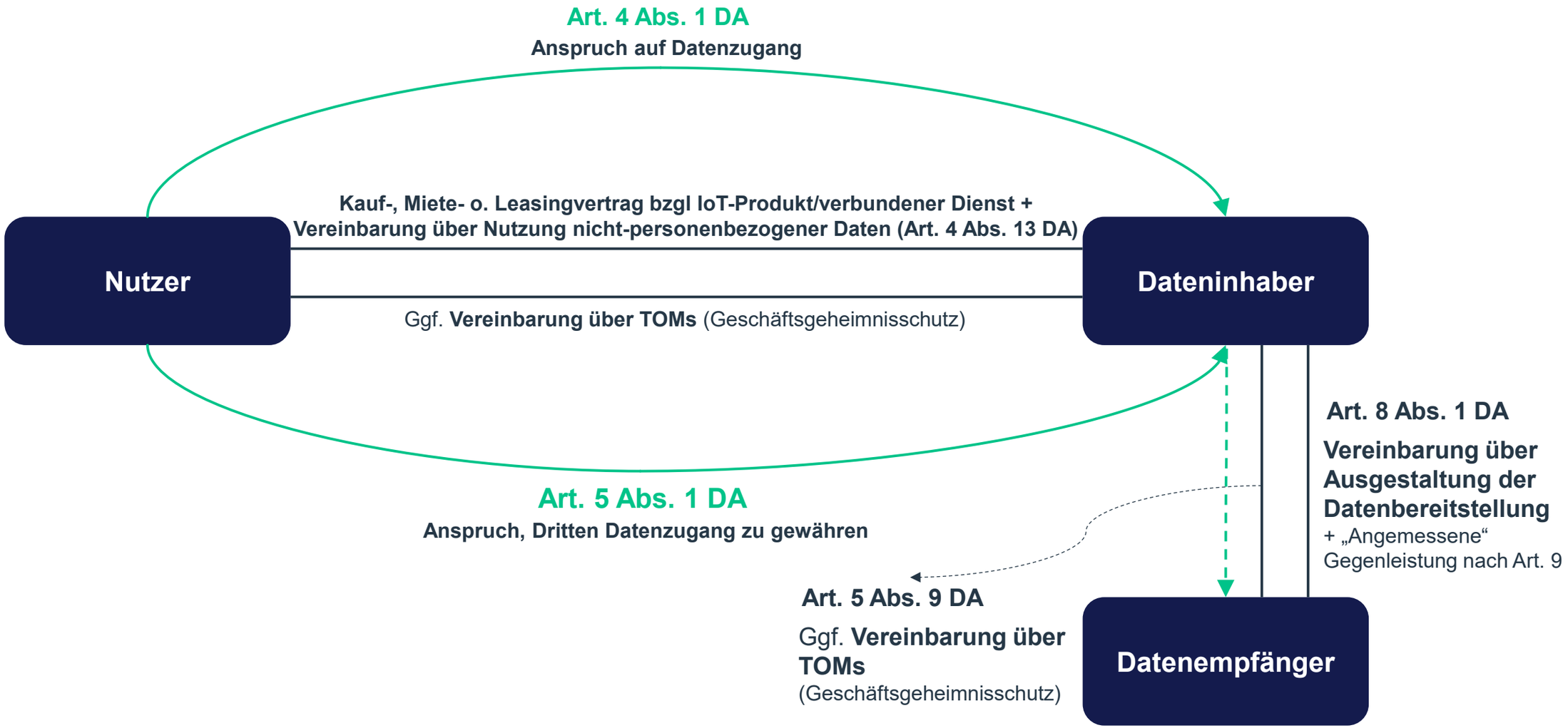
Sachlicher Anwendungsbereich
Datenzugang: Verbundener Dienst

<u>Wesentliche Eigenschaften von Verbundenen Diensten, Art. 2 Nr. 6 DA:</u>

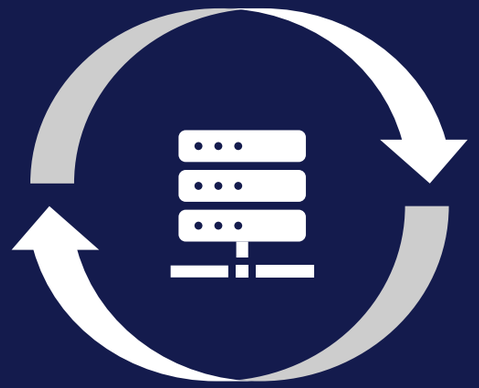
- <u>Kein</u> körperlicher Gegenstand, sondern „digitale“ Produkte (einschließlich Software)
- **Voraussetzung:** Vernetztes Produkt
- **Wechselseitiger Datenaustausch** zwischen dem vernetzten Produkt und dem verbundenen Dienst.
- Verbundener Dienst **beeinflusst die Funktionen, das Verhalten oder den Betrieb** des vernetzten Produkts.
- Durch Erbringung des verbundenen Dienstes gegenüber dem Nutzer des vernetzten Produkts wird der **Anbieter zum Dateninhaber**.

- **Entscheidend:** Inverkehrbringen auf dem Unionsmarkt
- **Ausgeschlossen:** Dienste in Bezug auf Konnektivität und Stromversorgung sowie Aftermarket-Dienste (z.B. zusätzliche Beratung, Analyse- und Finanzdienstleistungen sowie regelmäßige Reparatur- und Wartungsarbeiten).

DA: Vertragsbeziehungen



DA: Wechsel zwischen Datenverarbeitungsdiensten



Fairer Wechsel zw. Datenverarbeitungsdiensten

- Aufbrechen von
  - Lock-In-Effekt
  - Vendor-Lock-In
- Förderung eines fairen Wettbewerbs

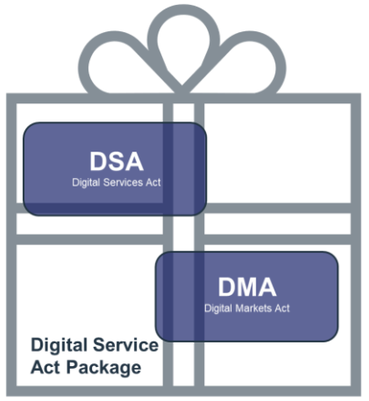
Anforderungen (Anbieter v. Datenverarbeitungsdiensten)

- Vertragsänderung (Recht des Kunden auf Wechseln)
- Beseitigung technischer Hürden für effektiven Wechsel
- Informationspflicht
- Transparenz
- Schrittweise Abschaffung der Wechselgebühren
  - 11. Januar 2024 → 12. Januar 2027: ermäßigte Gebühren
  - Ab 12. Januar 2027: keine Gebühren
- Umsetzung von Interoperabilitätsstandards

4 | Digital Services Act Package (DSA und DMA)

TaylorWessing

Digital Service Act (DSA)



Gegenstand

Einheitliche horizontale Regelungen zu Sorgfaltspflichten und Haftungsprivilegierung für Vermittlungsdienste

Ziel des DSA

Schaffung eines sicheren, vorhersehbaren und vertrauenswürdigen Online-Umfelds

→ umfassender Grundrechtsschutz von Nutzern

Wer ist betroffen?

Anbieter von digitalen Diensten, die Verbrauchern Waren, Dienstleistungen oder Inhalte vermitteln

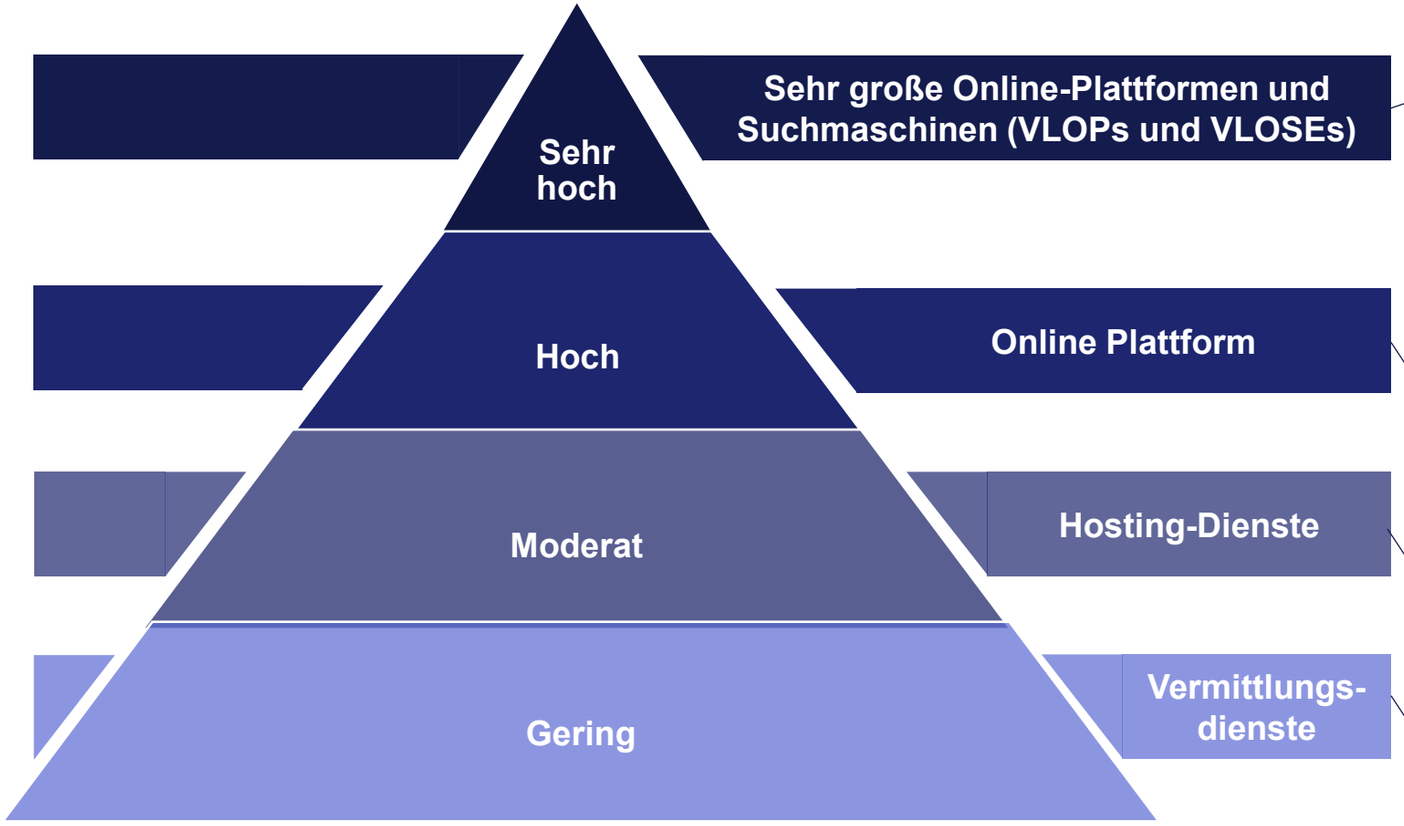
- Vermittlungsdienste
- Hosting-Dienste
- (Sehr große) Online-Plattformen oder Suchmaschinen)

Wann?

Trat am 16. November 2022 in Kraft;
seit dem **17. Februar 2024** vollumfassend anwendbar

Digitale-Dienste-Gesetz (DDG) setzt die ausgestaltungsbedürftigen Bestandteile des DSA in Deutschland um.

DSA: Maß an Sorgfaltspflichten



Risiko Verbreitung illegaler Inhalte und daraus resultierender Schäden besonders hoch
→ erreichen mehr als 10% der 450 Mio. Verbraucher in EU

z.B. Amazon, App Store (Apple), Booking

z.B. Online-Marktplätze, App-Stores, Social-Media-Plattformen, B2C-Online-Marktplätze

z.B. Cloud-Dienste und Webhosting

Bieten Netzinfrastruktur an: z.B. Internetanbieter und Domain-Registrierungsstellen

DSA: VLOPs und VLOSEs und Maßnahmen

Werden von der Kommission benannt (vgl. Art. 33 Abs. 4 DSA)

Very large online platforms (VLOPs):

- **AliExpress**
- **Amazon Store**
- **App Store (Apple)**
- **Aylo Freesites (18+ Dienst)**
- **Booking.com**
- **Facebook (Meta)**
- **Google Play**
- **Google Maps**
- **Google Shopping**
- **Instagram (Meta)**
- **LinkedIn**
- **NKL Associates s.r.o (18+ Dienst)**
- **Pinterest**
- **Shein**
- **Snapchat**
- **Technius (18+ Dienst)**
- **Temu**
- **TikTok**
- **WebGroup (18+ Dienst)**
- **Wikipedia**
- **X**
- **Youtube (Google)**
- **Zalando**

Very large online search engines (VLOSEs):

- **Bing**
- **Google Search**

Abrufbar unter: https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses

Maßnahmen des DSA

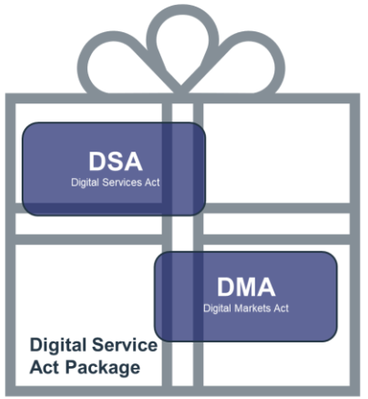
Leichtere Entfernung von illegalen Inhalten (z.B. Hassrede, Desinformation, gefälschte Produkte)

Verbot von „Dark Patterns“ und „Nudging“ → Schutz Autonomie der Nutzer

Höhere Transparenz bei Werbung

Höhere Anforderungen für Zugang zu B2C-Online Marktplätzen

Digital Markets Act (DMA)



Gegenstand

Regulierung und Stärkung digitaler Märkte durch das Verbot bestimmter wettbewerbs-beschränkender Praktiken

Ziel des DMA

Fairer Wettbewerb zwischen digitalen Plattformen unabhängig von ihrer Größe

→ Mehr Wahlmöglichkeit zwischen besseren Dienstleistungen zu gerechteren Preisen für Verbraucher

→ Marktbehauptungsmöglichkeit für Start-Ups und KMUs

Wer ist betroffen?

Sog. „**Gatekeeper**“ (Torwächter) mit bestimmten zentralen Plattformdiensten („**ZPD**“)

Wann?

Trat am 1. November 2022 in Kraft;
seit dem **2. Mai 2023** vollumfassend anwendbar

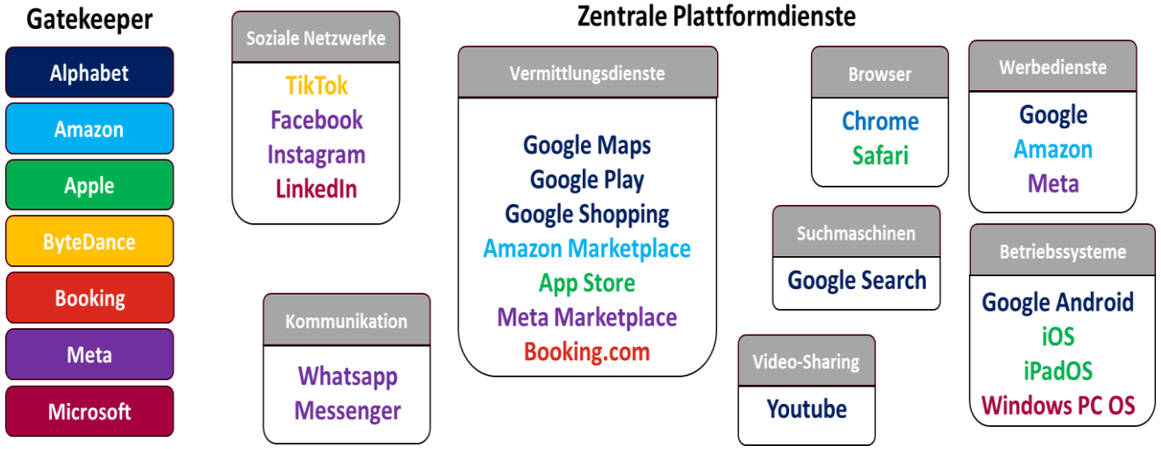
Sanktionen?

Bis zu 10 % des weltweiten Umsatzes des „Gatekeepers“ (bei wiederholten Zuwiderhandlungen bis zu 20%)

DMA: Gatekeeper und Maßnahmen

Kommission benennt Unternehmen zu „Gatekeeper“, wenn:

1. **Jahresumsatz über EUR 7,5 Mrd.** (letzte drei Geschäftsjahre) oder **über EUR 75 Mrd. Börsenwert**
2. **ZPD monatlich mehr als 45 Millionen aktive Nutzer (davon min. 10.000 gewerbliche EU-Nutzer)**
3. **ZPD in mindestens drei MS bereitgestellt**



Maßnahmen des DMA

Verhaltenskodex für „Gatekeeper“

Verbot unlauterer Praktiken

Beispiele unlauterer Praktiken:

- Rankings: Bevorzugung eigener Angebote
- Technische Blockierung von der Installation externer Anwendungen
- Entwickler hindern, Zahlungsplattformen Dritter für den Verkauf von Apps zu nutzen
- Software-Anwendungen vorinstallieren, ohne Möglichkeit diese zu deinstallieren

5 | EU-Cybersicherheit (NIS-2, DORA und CRA)

TaylorWessing

NIS-2 und DORA im Überblick

NIS-2-Richtlinie

- **Ziel:** EU-weite Mindeststandards für Cybersicherheit, um kritische und wichtige Unternehmen widerstandsfähiger zu machen (Art. 1 Abs. 1 NIS-2-RL)
- **Wer ist betroffen?** Öffentliche oder private Einrichtungen der in den Anhang I („**hohe Kritikalität**“) oder II („**sonstige kritische Sektoren**“)

  → Nicht nur „kritische Infrastrukturen“, sondern auch z.B. digitale Dienste, Lebensmittelproduktion etc.

- **Pflichten**
  - **Einführung von Risikomanagement-Maßnahmen** (Security by Design, Notfallpläne)
  - **Meldepflichten bei Sicherheitsvorfällen** (oft binnen 24 Stunden)
- **Räumlich:** in den EU-Mitgliedstaaten
- **Zeitlich:**
  - > Inkrafttreten: 16. Januar 2023
  - > Umsetzungsfrist: bis zum 18. Oktober 2024
  - > In D: **NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz** (zwischenzeitlich an Ampel-Aus gescheitert; im **Juli 2025** von neuem Bundeskabinett beschlossen)

Merke: NIS-2 will erreichen, dass Ausfall eines Unternehmens nicht gleich Versorgung ganzer Gesellschaftsbereiche gefährdet

„Cybersicherheits-zwillinge“

NIS-2: allgemein für Gesellschaft und Wirtschaft

DORA: spezifisch für den Finanzsektor (mit tlw. höheren Anforderungen)

Digital Operational Resilience Act (DORA)

- **Ziel:** Vertrauen in die Finanzmärkte stärken, indem man sicherstellt, dass diese selbst bei schweren Cyberangriffen oder Systemausfällen weiterlaufen (Art. 1 Abs. 1 DORA)
- **Wer ist betroffen?** Banken, Versicherungen, Zahlungsdienstleiter, Börsen etc.
- **Pflichten**
  - **Umfassendes IT-Risikomanagement**
  - **Überwachung der IT-Dienstleister** (Cloud-Anbieter etc.)
  - **Meldepflichten bei IT-Störungen**
  - **Regelmäßige Tests zur Widerstandsfähigkeit**
- **Räumlich:** in den EU-Mitgliedstaaten
- **Zeitlich:**
  - > Inkrafttreten: 16. Januar 2023
  - > Anwendungspflicht: seit **17. Januar 2025**

Merke: DORA will sicherstellen, dass Finanzmärkte auch dann stabil bleiben, wenn zentrale IT-Systeme durch Cyberangriffe oder Störungen unter Druck geraten

Cyber Resilience Act (CRA)

15.9.2022: Vorschlag der EU-Kommission für eine Verordnung über horizontale Anforderungen an die Cybersicherheit von Produkten mit digitalen Elementen (Cyber Resilience Act)

- Einführung von Sicherheitsanforderungen für ein breites Spektrum an **materiellen und immateriellen Produkten mit digitalen Elementen**, inklusive nicht-integrierter Software

11.12.2024 Inkrafttreten

11.09.2026 Meldepflichten

11.12.2027 Wirksamkeit

Anwendungsbereich

- Hersteller, Importeure und Händler, die ein Produkt mit digitalen Elementen auf den Markt bringen **dessen beabsichtigte oder vorhersehbare Verwendung eine logische oder physische Datenverbindung zu einem Gerät oder Netzwerk umfasst**
- Ausnahmen bspw. für gewisse medizinische Produkte oder Produkte für militärische Zwecke
- Kein SaaS
- Free and Open-Source Software nur bei gewerblicher Nutzung erfasst
- Der Begriff der Herstellers und der des Produkts mit digitalen Elementen werden weit verstanden

CRA: Pflichten der Hersteller

- **Design, Entwicklung und Produktion entsprechend Anhang I CRA,** z.B.
  - Produkte mit digitalen Elementen müssen so entworfen, entwickelt und produziert werden, dass sie ein **angemessenes Cybersicherheitsniveau** garantieren
  - Produkte mit digitalen Elementen sollen **ohne bekannte ausnutzbare Schwachstellen** geliefert werden
  - Produkte sollen mit einer **sicheren Standardkonfiguration** geliefert werden, die die Möglichkeit bietet, das Produkt in seinen ursprünglichen Zustand zurückzusetzen
- Cybersecurity **Risk Assessment,** um Sicherheitsrisiken zu minimieren
- Due Diligence bei Integration von Drittanbieterkomponenten
  - Dokumentationspflichten bevor das Produkt auf dem Markt platziert wird
- **Konformitätsprüfungsverfahren** (darauf folgend: CE-Zertifizierung + EU-Konformitätserklärung)
- Beifügen von Produktinformationen sowie Gebrauchsanweisungen
- **Meldepflichten,** bspw. an ENISA innerhalb von 24h nach Entdecken von Schwachstellen

CRA: Marktaufsichtsbehörde und Sanktionen

Marktaufsichtsbehörde

- Überwacht die effektive Umsetzung des Cyber Resilience Acts
- Konformitätsüberprüfung von Produkten, wenn diese ein erhebliches Sicherheitsrisiko darstellen

Sanktionen

- Bei Verletzung der essenziellen Sicherheitsanforderungen aus Anhang I bis zu **EUR 15.000.000** oder **2.5%** des weltweiten Umsatzes des vorangegangen Geschäftsjahres (Art. 64 Abs. 2 CRA)
- Bei Übermittlung falscher Informationen an die Marktaufsichtsbehörde bis zu **EUR 5.000.000** oder **1%** des weltweiten Umsatzes des vorangegangen Geschäftsjahres (Art. 64 Abs. 4 CRA)
- Im Falle anderweitiger Verstöße bis zu **EUR 10.000.000** oder **2%** des weltweiten Umsatzes des vorangegangenen Geschäftsjahres (Art. 64 Abs. 3 CRA)

6 | EU Accessibility Act

TaylorWessing

European Accessibility Act (1)

Kernidee

- EU-weiter Standard für Barrierefreiheit von Produkten und Dienstleistungen
- Nur B2C, aber B2B - Angebot muß Teilnahme von Verbrauchern ausschließen

Wer ist betroffen

- Hersteller, Importeure und Händler bestimmter **Produkte und Dienstleistungen**, z.B.
  - **Produkte**: Computer, Smartphones, Bankautomaten, E-Books und Ticketautomaten
  - **Dienstleistungen**: Online Shops, E-Banking, elektronische Kommunikationsdienste, Personenbeförderungstickets

Ziel

- Menschen mit Einschränkungen sollen in europäischem Binnenmarkt selbständig am digitalen Leben teilnehmen können

Anwendungsbereich

- Inkrafttreten: 28. Juni 2019
- Umsetzungspflicht: bis 28. Juni in nationales Recht
- Anwendung der Vorschriften seit **28. Juni 2025** (tlw. mit Übergangsfristen für bereits in Verkehr gebrachte Produkte)

Umsetzung in Deutschland

Kategorie	Gesetzliche Grundlage	Anwendungsbereich	Ausnahmen
Private Anbieter	**BFSG** (seit 2025 anwendbar)	Websites, Apps, E-Commerce, Automaten etc.	Kleinst-unternehmen
Öffentliche Anbieter	**BGG + BITV 2.0**, ergänzt durch BFSG	Digitale Angebote öffentlicher Stellen	Keine speziellen Ausnahmen erwähnt

European Accessibility Act (2) – Maßnahmen

Allgemeine funktionale Anforderungen

- Informationen müssen **wahrnehmbar, bedienbar, verständlich und robust** gestaltet sein
- Barrierefreie Schnittstellen: etwa taktile, sprachbasierte oder alternative Bedienmöglichkeiten
- Kompatibilität mit Hilfsmitteln (Screenreader, Braillezeilen, Spracherkennungssoftware)
- **Barrierefreiheitserklärung** mit Angaben über Konformität und Kontaktmöglichkeiten
- **Melde- und Nachweispflichten** gegenüber Aufsichtsbehörden

Digitale Dienstleistungen

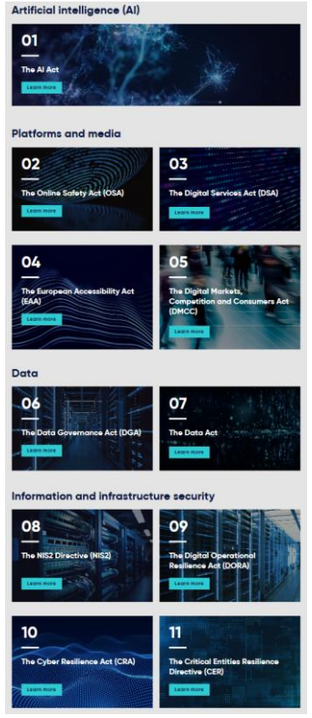
- Texte, Bilder, Formulare etc. müssen **maschinenlesbar** sein
- Videos mit **Untertitel und Audiodeskriptionen**
- Nutzerführung klar und konsistent, keine Barrieren in Bestell- oder Zahlungsvorgängen

Produkte

- **Bedienung über verschiedene Sinne** möglich (visuell, akustisch, taktil)
- Klar erkennbare Bedienelemente, auch mit Hilfsmitteln nutzbar
- Bereitstellung einer **barrierefreien Gebrauchsanleitung**

Europäische Digitalgesetze – nochmal zum Nachschauen

Digital and data regulation guide



Home - Digital, data and consumer regulation

Digital legislation in a page

With so much complex digital legislation coming in in the EU and UK, it can be hard to navigate even the essentials. We've produced a set of one-page overviews of key legislation at the top of the agenda for 2025, covering:

- EU AI Act
- EU Digital Services Act
- EU Data Act
- EU Data Governance Act
- EU Cyber Resilience Act
- EU NIS2 Directive
- EU Machinery Regulation
- EU Gigabit Infrastructure Act
- EU European Health Data Space proposal
- UK Online Safety Act.

You can see table summaries of other aspects of the EU AI Act here, and of the UK Online Safety Act here. You may also be interested in our Digital Legislation Tracker and our Digital and data regulation guide.

Digital legislation in a page

Q&A

TaylorWessing

Ihr Ansprechpartner

Axel Freiherr von dem Bussche ist Fachanwalt für Informationstechnologierecht in der Praxisgruppe Technology, Media & Telecoms. Er begleitet Mandanten in nationalen und internationalen Digital- und Datenschutzprojekten und ist ausgewiesener IT-Rechts und DSGVO-Experte.

Axel von dem Bussche steuert mit seiner langjährigen Erfahrung und herausragenden Expertise Mandanten auf der Anbieter- und Anwenderseite routiniert durch komplexe, internationale Transaktionen, Vertragsgestaltungen und Regulierungsfragen. Er begleitet Konzerne bei der Transformation zu digitalen und globalen Geschäftsmodellen, unterstützt Unternehmen bei der Implementierung von KI - und Datenschutzvorschriften, ist strategischer Berater der Geschäftsleitung zur Compliance in der Digitalisierung und führt Verhandlungen mit den zuständigen Aufsichtsbehörden.

Sprachen

- Deutsch, Englisch, Französisch

„Der Datenschutzspezialist Axel von dem Bussche berät namhafte Mandanten in datenschutzrechtlichen Fragen (…). Zudem vertritt er Mandanten in Verfahren auf regionaler und nationaler Ebene gegen Datenschutzaufsichtsbehörden.“; „Er hat alle neuen Updates, ist sehr mandatsorientiert und analysiert schnell neue Gesetze“, Mandant, Chambers Europe 2021-2024, Chambers Germany 2025

Ausgezeichnet als “Thought Leader” für Datenschutz in Deutschland, Who’s Who Legal 2025

Hervorgehobener Anwalt für Datenschutz, Chambers Europe 2019 - 2024

Empfohlen für Informationstechnologie und Datenschutz “einer der Besten, absoluter Stratege“, Mandant, „sehr starke Mandantenorientierung, Verhandlungskompetenz u. Durchsetzungsstärke“, „schlechthin der Experte für den Datenschutz, exzellente Fachkenntnisse sowie Verhandlungsgeschick“ „exzellente Beratungsleistung u. Fachkenntnisse gepaart mit einer ausgeprägten Mandantenorientierung“, „bester Anwalt in Dtl. bei Litigation-Fällen im Datenschutz“, Mandant; „sehr umtriebig, äußerst stark“, „absoluter Kenner der Branche“, „fordert auffallend gut Nachwuchs“, „angenehmen u. sehr versiert“, Wettbewerber; JUVE 2015/2016- 2024/2025

Führender Name für IT und Digitalisierung, The Legal 500 2021 - 2025

Führender Anwalt für Datenschutz Kanzleimonitor (diruj) 2020/2021 - 2023/24

Top-100-Anwälte Deutschlands, Kanzleimonitor (diruj) 2023/24

TOP Anwalt für Datenschutzrecht, WirtschaftsWoche 2019-2023

Herausragender Anwalt, Thomson Reuters 2022

Geführt in der Bestenliste als ein international führender Anwalt für Datenschutz und IT, Who’s Who Legal 2019-2024

Hervorgehoben als "Anwalt des Jahres" 2024 und Best Lawyer für IT-Recht, Best Lawyers in Germany, Handelsblatt 2018 - 2024

Dr. Axel Frhr. von dem Bussche, LL.M. (L.S.E.)

Partner
Hamburg

+49 40 36803-229
a.bussche@taylorwessing.com

Beratungsschwerpunkte

- Informationstechnologie/ Telekommunikation
- Datenschutz
- Urheber- & Medienrecht
- Litigation & Dispute Resolution
- Technology, Media & Communications

Europa > Mittlerer Osten > Asien

taylorwessing.com