DIE AKTUELLE EU-GESETZGEBUNG IM BEREICH DIGITALISIERUNG UND DATENWIRTSCHAFT

MÖGLICHE AUSWIRKUNGEN FÜR FORSCHUNGS- UND ENTWICKLUNGSPROJEKTE – EINE ÜBERSICHT

Erstellt im Rahmen der vom Bundesministerium für Wirtschaft und Klimaschutz beauftragten Begleitforschungen zu den Technologieprogrammen „KI-Innovationswettbewerb“ und „Smarte Datenwirtschaft“

IMPRESSUM

Erstellt im Rahmen der vom Bundesministerium für Wirtschaft und Klimaschutz beauftragten Begleitforschungen zu den Technologieprogrammen „KI-Innovationswettbewerb“ und „Smarte Datenwirtschaft“

AUTOREN
Sebastian Straub
Christoph Bogenstahl

HERAUSGEBER
Peter Gabriel, Dr. Steffen Wischmann
Begleitforschung Smarte Datenwirtschaft und
Begleitforschung KI-Innovationswettbewerb
Institut für Innovation und Technik (iit)
in der VDI / VDE Innovation + Technik GmbH
Steinplatz 1
10623 Berlin
gabriel@iit-berlin.de, wischmann@iit-berlin.de

VERÖFFENTLICHUNG
Februar 2023

GESTALTUNG
LHLK Agentur für Kommunikation GmbH
Hauptstraße 28
10827 Berlin

BILDER
sdecoret – stock.adobe.com (Titel)

EINLEITUNG

Die Europäische Kommission hat am 9. März 2021 ihre Zielvorstellung für die digitale Transformation Europas bis zum Jahr 2030 formuliert (EU Kommission 2021). Darin beschreibt sie eine auf den Menschen ausgerichtete und nachhaltige Vision für eine digitale Gesellschaft. Ein wichtiger Baustein auf dem Weg in die „digitale Dekade" ist die Europäische Datenstrategie (EU Kommission 2020a). Sie zielt darauf ab, einen Binnenmarkt für Daten zu schaffen, der die globale Wettbewerbsfähigkeit und Datensouveränität Europas gewährleistet. Daneben werden im Rahmen der Strategie „Künstliche Intelligenz für Europa" konzeptionelle Vorschläge für Exzellenz und Vertrauen in Künstliche Intelligenz (KI) beschrieben (EU Kommission 2018). Die Verwirklichung eines daten- und KI-getriebenen Binnenmarkts soll nicht nur durch die Förderung von Spitzentechnologien, sondern auch durch die Schaffung von regulatorischen Rahmenbedingungen erreicht werden. Zur Umsetzung dieser strategischen Ziele werden in einem beachtlichen Tempo Gesetzgebungsvorhaben auf den Weg gebracht, die ebenso rasch in der Praxis umgesetzt werden sollen. Dies stellt insbesondere Forschungs- und Entwicklungsprojekte, die mit der Umsetzung von daten- und KI-basierten Technologien befasst sind, vor erhebliche Herausforderungen.

Die vorliegende Publikation gibt eine Übersicht über die fünf aktuellen Gesetzgebungsaktivitäten der Europäischen Union im Bereich Digitalisierung und Datenwirtschaft:

1. Artificial Intelligence Act
2. Data Governance Act
3. Data Act
4. Digital Services Act
5. Digital Markets Act

Diese Analyse wurde im Rahmen der Begleitforschungsaufträge des BMWK zu den Technologieprogrammen „KI-Innovationswettbewerb" und „Smarte Datenwirtschaft" erstellt. Daher werden bei der Darstellung der Rechtsakte jeweils schwerpunktmäßig die folgenden Fragen in Bezug auf die in den Programmen geförderten FuE-Projekte adressiert:

- Worum geht es? (Anwendungsbereich)
- Wen betrifft die Regelung? (Adressatenkreis)
- Gibt es Sanktionsmöglichkeiten?
- Was sind die Auswirkungen auf FuE-Projekte?

Im Anhang findet sich für die betrachteten Rechtsakte ein Glossar zentraler Begriffe sowie eine Kurzübersicht zu deren Inhalten und Auswirkungen auf FuE-Projekte.

Die Darstellungen berücksichtigen den aktuellen Stand der jeweiligen Gesetzgebungsverfahren (Stand Januar 2023).

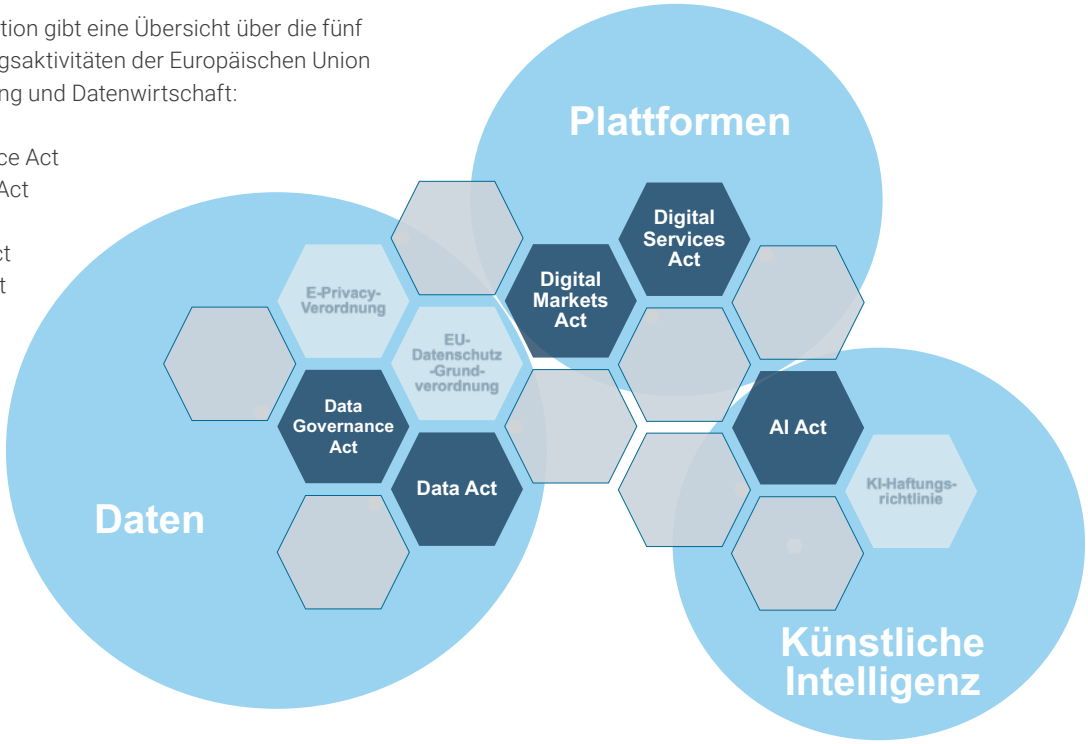


Abbildung 1: Aktuelle EU-Gesetzgebung im Bereich Digitalisierung und Datenwirtschaft

INHALT

01

1 ARTIFICIAL INTELLIGENCE ACT (AI ACT)

Mit der KI-Verordnung (Artificial Intelligence Act bzw. AI Act) wird ein EU-weit einheitlicher Rechtsrahmen für die Entwicklung, Vermarktung und Verwendung Künstlicher Intelligenz geschaffen (Rat der Europäischen Union 25.11.2022). Die Initiative für den Legislativvorschlag geht auf die 2018 veröffentlichte Europäische KI-Strategie zurück (EU Kommission 2018). Vorarbeiten der Verordnung beruhen auf den Erkenntnissen des Weißbuchs zur Künstlichen Intelligenz (EU Kommission 2020b). Dort wurden u. a. politische Optionen aufgezeigt, wie die Nutzung von KI gefördert und mögliche Risiken der Technologie eingedämmt werden können. Insbesondere der Ansatz eines risikobasierten Regulierungssystems und die Einteilung in Risikoklassen findet sich in dem Verordnungsentwurf wieder (siehe Abschnitt 1.3).

1.1 Anwendungsbereich

Die Verordnung stellt allgemeine Regeln für das Inverkehrbringen, die Inbetriebnahme und die Verwendung von Systemen der Künstlichen Intelligenz (sogenannte KI-Systeme) auf. Lange ungeklärt und im Gesetzgebungsprozess intensiv diskutiert war die Frage, wie der Begriff „Künstliche Intelligenz" rechtssicher definiert und zugleich eine ausreichende Flexibilität im Hinblick auf künftige technologische Entwicklungen bewahrt werden kann. Der erste Verordnungsvorschlag definierte den Begriff KI-System noch sehr weit. Dies hätte unter Umständen dazu geführt, dass die KI-Verordnung auch auf herkömmliche Software anwendbar gewesen wäre. Zuletzt wurde der Fokus stärker auf die funktionalen Merkmale von KI gelegt und dabei auf Aspekte wie die Lern-, Denk- oder Modellierungsfähigkeiten abgestellt, die KI von einfacheren Softwaresystemen und Programmieransätzen unterscheiden.[1] Die im aktuellen Kompromissvorschlag gefundene Definition (Stand Januar 2023) setzt als zentrales Merkmal von KI-Systemen voraus, dass das System Techniken des maschinellen Lernens und/oder logik- und wissensbasierte Ansätze verwendet. Als Ansätze des maschinellen Lernens werden beispielhaft Deep Learning mit neuronalen Netzen, statistische Lern- und Inferenztechniken (einschließlich logistischer Regression, Bayes'sche Schätzung) sowie Such- und Optimierungsmethoden aufgeführt.[2] Als Beispiele für Logik- und wissensbasierte Ansätze werden Wissensrepräsentation, induktive (logische) Programmierung, Wissensbasen, Inferenz- und deduktive Maschinen, (symbolisches) Schließen, Expertensysteme sowie Such- und Optimierungsmethoden genannt. Obwohl die Definition im Laufe des Gesetzgebungsverfahrens präzisiert wurde, können sich Rechtsunsicherheiten bei der Interpretation der Begriffe ergeben. Um einheitliche Bedingungen für die Durchführung der Verordnung in Bezug auf diese Techniken und Ansätze zu gewährleisten, wird die EU-Kommission daher ermächtigt, Durchführungsrechtsakte[3] zu erlassen, um die technischen Elemente dieser Ansätze unter Berücksichtigung der Markt- und Technologieentwicklungen zu präzisieren. Hierdurch soll außerdem sichergestellt werden, dass die KI-Verordnung in Bezug auf neue technologische Entwicklungen flexibel und zukunftssicher bleibt.

1 Erwägungsgrund 6 der KI-Verordnung.
2 Vgl. Erwägungsgrund 6a der KI-Verordnung.
3 Ein Durchführungsrechtsakt ist ein Rechtsakt ohne Gesetzescharakter, in dem detaillierte Vorschriften für die einheitliche Durchführung verbindlicher Rechtsakte der EU festgelegt werden.

1.2 Adressatenkreis

Durch die Verordnung werden vorrangig Anbieter von KI-Systemen in die Pflicht genommen. Als Anbieter gelten natürliche oder juristische Personen, aber auch Behörden, Einrichtungen oder sonstige Stellen, die ein KI-System entwickeln oder entwickeln lassen, mit dem Ziel, das System in Verkehr zu bringen oder in Betrieb zu nehmen. Daneben gilt die Verordnung auch für Nutzende von KI-Systemen, also solche Akteure, die ein KI-System in eigener Verantwortung verwenden. Neben Anbietern und Nutzenden werden auch weitere Beteiligte entlang der KI-Wertschöpfungskette adressiert. In diesem Zusammenhang sind etwa Pflichten für Akteure vorgesehen, die mit KI-Systemen von Unternehmen außerhalb der EU handeln oder diese in die EU einführen wollen.

1.3 Risikoklassen

Die KI-Verordnung sieht insgesamt vier Risikoklassen vor (unannehmbares, hohes, geringes und minimales Risiko). KI-Systeme mit einem unannehmbaren Risiko unterliegen einem Verbot. KI-Systeme mit einem hohen Risiko müssen hohe Compliance-Vorgaben erfüllen. Systeme, die mit einem geringen oder minimalen Risiko assoziiert sind, müssen Transparenzvorgaben erfüllen bzw. unterliegen keinen regulatorischen Vorgaben.

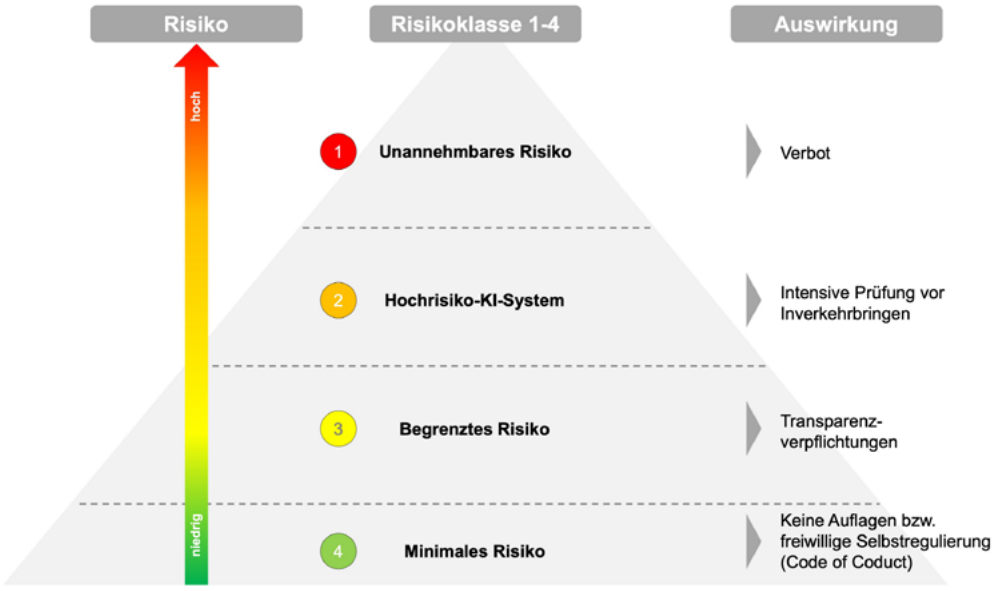


Abbildung 2: Übersicht zu Risikoklassen von KI-Systemen

1.3.1 RISIKOKLASSE 1: UNANNEHMBARES RISIKO

Bestimmte KI-Praktiken werden mit unannehmbaren Risiken in Verbindung gebracht und unterliegen einem Verbot. Hierzu zählen Techniken, die darauf ausgerichtet sind, Personen zu manipulieren oder die Schwäche oder Schutzbedürftigkeit bestimmter (vulnerabler) Personengruppen auszunutzen. Dabei muss das KI-System das Verhalten dieser Personen oder Personengruppe

derart beeinflussen, dass Schäden (physischer oder psychischer Art) hervorgerufen werden. Untersagt ist zudem das Inverkehrbringen, die Inbetriebnahme oder die Verwendung von KI-Systemen durch Behörden zur Bewertung oder Klassifizierung der Vertrauenswürdigkeit natürlicher Personen („Social Scoring") sowie der Einsatz von biometrischen Echtzeit-Fernidentifizierungssystemen in öffentlich zugänglichen Räumen zu Zwecken der Strafverfolgung.

1.3.2 RISIKOKLASSE 2: HOCHRISIKO-KI-SYSTEME

Im Zentrum der Verordnung steht die Regulierung von sogenannten Hochrisiko-KI-Systemen. Dabei handelt es sich um Systeme, deren Ausfall oder Störung besonders schwerwiegende Folgen für die Sicherheit, Gesundheit und die Grundrechte von natürlichen Personen haben würde. Solche Hochrisiko-KI-Systeme sollen nur dann auf den Markt gebracht oder in Betrieb genommen werden, wenn sie bestimmte, nachprüfbare Anforderungen erfüllen. Die Klassifikation als Hochrisiko-KI-System betrifft dabei drei Fälle:

Fall 1: „KI ist Produkt oder sicherheitsrelevanter Produktbestandteil."

Anhang-II-Systeme (KI-System ist Produkt oder Sicherheitskomponente eines Produkts und unterliegt einer EU-Sicherheitsregulierung): Anhang II Abschnitt A der KI-Verordnung enthält einen Katalog von einschlägigen EU-Rechtsakten. Dabei handelt es sich vorrangig um Richtlinien und Verordnungen, welche das Inverkehrbringen oder die Inbetriebnahme von besonders sicherheitsrelevanten Produkten regeln (z. B. Maschinen, Spielzeug oder medizinische Geräte). KI-Systeme, die als Produkt oder Produktbestandteil aufgrund einer dieser Rechtsakte einer Konformitätsbewertung durch Dritte unterliegen, gelten automatisch als Hochrisiko-KI-Systeme.

Fall 2: „KI ist Produkt oder sicherheitsrelevanter Produktbestandteil – in Bereichen mit bereits bestehenden Prüf- und Zulassungsverfahren."

Anhang II enthält in Abschnitt B eine Liste mit weiteren EU-Rechtsakten. Fällt das KI-System in den Regelungsbereich der dort genannten Richtlinien oder Verordnungen, findet die KI-Verordnung weitestgehend keine Anwendung. Der Grund hierfür ist, dass in den dort adressierten Bereichen (z. B. Typengenehmigung von Kraftfahrzeugen oder Sicherheit in der zivilen Luftfahrt) bereits bestehende Prüf- und Zulassungsverfahren bestehen. Der Gesetzgeber will aus diesem Grund nicht unnötig in bereits etablierte und ausdifferenzierte Regelungssysteme eingreifen. Auch wenn KI-Systeme, die unter Anhang II Abschnitt B fallen, vom Anwendungsbereich vorerst ausgenommen sind, sollten Hersteller in diesem Bereich die Vorgaben der KI-Verordnung künftig dennoch berücksichtigen. Denn die bereichsspezifischen Sicherheitsregulierungen werden so angepasst, dass die Mindestanforderungen der KI-Verordnung bei der Fortschreibung dieser Rechtsakte berücksichtigt werden müssen. Somit ergeben sich zumindest mittelbare Auswirkungen auf die Ausgestaltung dieser Produkte bzw. Produktbestandteile.

Fall 3: „Einsatz von KI in besonders sensiblen Bereichen."

KI-Systeme gelten als potenziell hochriskant, wenn sie in einem der in Anhang III aufgeführten Bereiche eingesetzt werden sollen. Hierzu gehört u. a. der Einsatz in kritischen Infrastrukturen, in den Bereichen Bildung, Beschäftigung, Strafverfolgung, Migration oder Rechtspflege. Von einem hohen Risiko ist aber nur dann auszugehen, wenn die Ausgabe des Systems mit einem tatsächlichen Risiko für die Gesundheit, Sicherheit oder Grundrechte von Personen verbunden ist. Ist die

Ausgabe der KI für die zu treffende Entscheidung nur nebensächlich, liegt kein Hochrisiko-KI-System vor. KI-Systeme, die aufgrund ihrer technischen Funktionalität mit einem besonders hohen Risiko verbunden sind, wie beispielsweise die biometrische Identifizierung von natürlichen Personen, gelten ebenfalls als hochriskant.

Bereiche von Hochrisiko-KI-Systemen nach Anhang III (EU Kommission 2022):

- Kritische Infrastrukturen, bei Gefährdung von Leben und Gesundheit von Personen (z. B. im Verkehr)
- Schul- oder Berufsausbildung, wenn Beeinträchtigung des Zugangs zu Bildungsangeboten droht (z. B. bei Hochschulzulassungsverfahren oder der Bewertung von Prüfungen)
- Beschäftigung, Personalmanagement und Zugang zu selbstständiger Tätigkeit (z. B. Software zur Auswertung von Lebensläufen für Einstellungsverfahren, Bewertung der Leistung von Beschäftigten)
- Zentrale private und öffentliche Dienstleistungen (z. B. Bewertung der Kreditwürdigkeit, Zugang zu Sozialleistungen des Staates)
- Strafverfolgung, die in die Grundrechte der Menschen eingreifen könnte (z. B. Auswertung der Echtheit von Beweismitteln)
- Migration, Asyl und Grenzkontrolle (z. B. Überprüfung der Echtheit von Reisedokumenten)
- Biometrische Identifizierung und/oder algorithmengestützte Kategorisierung von Personen, beispielsweise im Rahmen der Strafverfolgung oder Grenzkontrolle, Migration, Asylverfahren, Straffälligkeitsüberprüfung/Überprüfung von Bewährungsauflagen
- Rechtspflege (z. B. bei der Auslegung von Rechtsvorschriften)

1.3.2.1 Mindestanforderungen an Hochrisiko-KI-Systeme

Hochriskante KI-Systeme müssen bestimmten Mindestanforderungen genügen. Die Anforderungen dienen vorrangig der Minimierung von Risiken, berücksichtigen aber auch ethische Aspekte sowie Aspekte der Transparenz und Nachvollzierbarkeit von Künstlicher Intelligenz. Zu den Mindestanforderungen gehören u. a.

- Einrichtung eines Risikomanagementsystems, das eine Risikobewertung beinhaltet und Maßnahmen zur Risikominimierung oder -beseitigung vorsieht,
- Sicherstellung der Datenqualität, insbesondere durch Qualitätsvorgaben für Trainings-, Validierungs- und Testdatensätze,
- Technische Dokumentation als Nachweis darüber, wie die Mindestanforderungen sichergestellt werden,
- Automatische Protokollierung von Vorgängen und Ereignissen während des Betriebs,
- Einhaltung von Transparenzpflichten, damit Nutzende die Ergebnisse des KI-Systems interpretieren und verwenden können,
- Bereitstellung einer für den Nutzenden verständlichen Gebrauchsanweisung,
- Pflicht, das Hochrisiko-KI-System so zu entwickeln und zu konzipieren, dass eine menschliche Aufsicht für die Dauer der Verwendung sichergestellt ist,
- Sicherstellung der Robustheit, Sicherheit und Genauigkeit des KI-Systems.

1.3.2.2 Pflichten für Anbieter und Nutzende von Hochrisiko-KI-Systemen

Anbieter von Hochrisiko-KI-Systemen müssen zunächst die Einhaltung der Mindestanforderungen für Hochrisiko-KI-Systeme (siehe oben) sicherstellen. Eine zentrale Pflicht besteht darüber hinaus in der Einrichtung eines Qualitätsmanagementsystems, welches durch konkret zu benennende Verfahren und Anweisungen die Einhaltung der Vorgaben der Verordnung gewährleistet. Dies umfasst Aspekte wie die Darstellung von Untersuchungs-, Test- und Validierungsverfahren oder Ausführungen zum Datenmanagement. Zudem müssen Prozesse zur Beobachtung des KI-Systems nach Inverkehrbringen sowie Verfahren zur Meldung von schwerwiegenden Vorfällen und Fehlfunktionen etabliert werden. Zugunsten von kleineren Anbietern ist eine Verhältnismäßigkeitsklausel vorgesehen. Danach soll die Umsetzung der genannten Vorgaben in einem angemessenen Verhältnis zur Größe der Organisation des Anbieters stehen.

Des Weiteren besteht die Pflicht zur Durchführung eines Konformitätsbewertungsverfahrens. Bei Anhang-III-KI-Systemen genügt ein internes Konformitätsbewertungsverfahren (ausgenommen sind biometrische Fernidentifizierungssysteme). Bei Anhang-II-KI-Systemen (Abschnitt A) befolgt der Anbieter die einschlägigen Konformitätsbewertungsverfahren, die nach den dort genannten Rechtsakten erforderlich sind. Wird eine entsprechende Konformitätsbewertung erfolgreich durchlaufen, erstellen die Anbieter eine EU-Konformitätserklärung und bringen das CE-Kennzeichen an. Zudem besteht die Verpflichtung, das Hochrisiko-KI-System in einer öffentlich einsehbaren EU-Datenbank zu registrieren. Die Datenbank wird nach In-Kraft-Treten der Verordnung von der EU-Kommission eingerichtet.

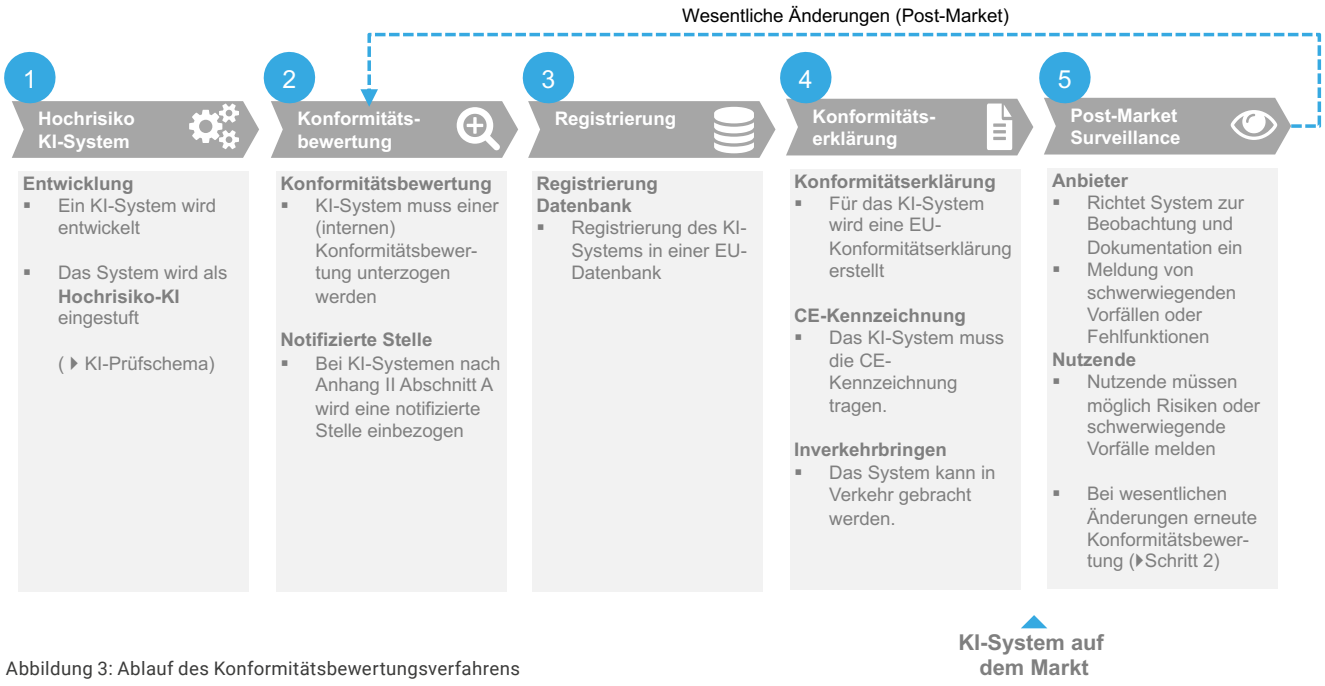


Abbildung 3: Ablauf des Konformitätsbewertungsverfahrens

1.3.3 RISIKOKLASSE 3: BEGRENZTES RISIKO

Für KI-Systeme mit spezifischen Manipulationsrisiken müssen – unabhängig davon, ob sie als hochriskant eingestuft werden – Transparenzpflichten eingehalten werden. Personen sollen beispielsweise informiert werden, wenn sie mit einem KI-System interagieren, beispielsweise im Rahmen der Bearbeitung von Kundenanfragen (z. B. Chat-Bots). Hiervon kann abgesehen werden, wenn offensichtlich ist, dass es sich bei dem Gegenüber um ein Softwaresystem handelt. Eine Mitteilungspflicht besteht auch gegenüber Verwendern von Emotionserkennungssoftware oder Systemen der biometrischen Kategorisierung. Zudem sollen KI-Systeme, die Bild-, Audio- oder Video-Inhalte von Personen, Gegenständen, Orten oder Ereignissen erzeugen oder manipulieren, gekennzeichnet werden. Der Verordnungsgeber hat damit vor allem sogenannte „Deepfakes" im Blick. Diese Art von KI-Systemen sind in der Lage, Foto-, Video- oder Audioaufnahmen so zu verändern, dass sie von authentischen Inhalten kaum zu unterscheiden sind.

1.3.4 RISIKOKLASSE 4: MINIMALES RISIKO

Für KI-Systeme mit minimalem Risiko gelten keine Auflagen. Anbieter solcher Systeme können sich aber freiwillig an Verhaltenskodizes orientieren.

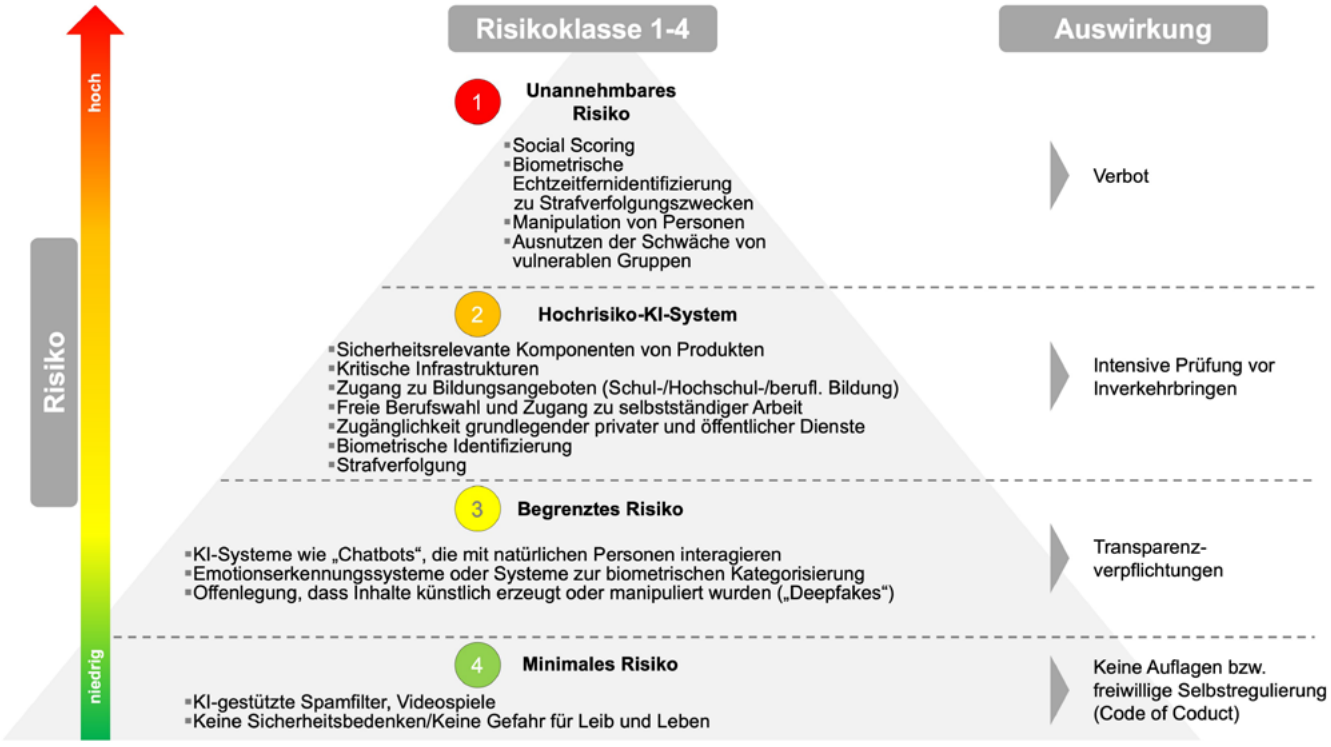


Abbildung 4: Die Risikoklassen 1 bis 4 der KI-Verordnung mit Beispielen und Auswirkungen

1.4 Sonderfall: General Purpose AI

Im Laufe des Legislativprozesses kam es zu einer Anpassung der KI-Verordnung dahingehend, dass für KI-Systeme ohne vorfestgelegten Einsatzzweck (allgemeine KI-Systeme, general purpose AI systems) Sonderregelungen geschaffen werden. Damit will der Verordnungsgeber der Komplexität der KI-Wertschöpfungskette Rechnung tragen und Anbieter entlasten, deren KI-System auf allgemeine Aufgaben wie Bild- und Spracherkennung, Audio- und Videogenerierung, Mustererkennung, Beantwortung von Fragen und Übersetzung mit allgemeinem Verwendungszweck ausgerichtet ist. Kennzeichnend für derartige KI-Systeme ist, dass diese in einer Vielzahl von Kontexten verwendet werden können und damit keinen vordefinierten Einsatzzweck aufweisen. Denkbar ist aber auch, dass derartige Systeme in Produkte oder Sicherheitskomponenten integriert werden, die als hochriskant einzustufen wären. Lange war umstritten, wie allgemeine KI-Systeme regulatorisch behandelt werden sollen. Nach dem derzeit vorliegenden Kompromissvorschlag (Stand Januar 2023) sollen die Regeln für Hochrisiko-KI-Systeme teilweise auch für allgemeine KI-Systeme gelten. Allerdings soll es zu keiner direkten Anwendung der Mindestanforderungen kommen. Stattdessen wird die EU-Kommission zum Erlass von delegierten Rechtsakten befugt, welche näher spezifizieren, wann und in welchem Umfang die Vorgaben für Hochrisiko-KI-Systeme auch für allgemeine KI-Systeme gelten sollen.

1.5 Durchsetzung und Sanktionen

Das Einhalten der Anforderungen der KI-Verordnung wird künftig behördlich überwacht. Hierfür sollen die Mitgliedstaaten entsprechende Aufsichtsbehörden schaffen. Ob diese Behörde in Deutschland neu geschaffen oder an bereits bestehende Institutionen (bspw. an das BSI) angegliedert wird, ist derzeit noch nicht absehbar. Anbieter von Hochrisiko-KI-Systemen müssen auf Verlangen der zuständigen Behörde in der Lage sein, die Konformität des KI-Systems mit den Anforderungen der Verordnung nachzuweisen. Im Rahmen der Überprüfung ist die Behörde berechtigt, alle Informationen und Unterlagen zu verlangen, die im Rahmen des Prüfverfahrens erforderlich sind. Dies umfasst auch den Zugang zu den automatisiert erzeugten Protokollen, soweit diese der Kontrolle des Anbieters unterliegen. Verstöße können mit Sanktionen geahndet werden. Diese sollen „wirksam, verhältnismäßig und abschreckend“ sein. Eine Verhängung von Bußgeldern in Höhe von 30 Millionen Euro oder sechs Prozent des gesamten weltweiten Jahresumsatzes können bei Verstößen gegen verbotene KI-Praktiken verhängt werden. Bei Missachtung der übrigen Anforderungen sind Bußgelder in Höhe von 20 Millionen Euro oder vier Prozent des gesamten weltweiten Jahresumsatzes möglich. Bei der Verhängung von Sanktionen sollen die Aufsichtsbehörden die Größe und die Interessen von KMU, einschließlich neu gegründeter Unternehmen, und deren wirtschaftliche Lebensfähigkeit berücksichtigen.

1.6 KI-Reallabore

Als einen Baustein der Innovationsförderung sieht die KI-Verordnung die Möglichkeit der Einrichtung von Reallaboren (regulatory sandboxes) vor. Im Rahmen dieser Experimentierräume soll die Entwicklung, Schulung, Erprobung und Validierung innovativer KI-Systeme vorangetrieben werden. Die sich ergebenden Spielräume sind jedoch insgesamt überschaubar. Die KI-Reallabore sollen durch die zuständigen Behörden der Mitgliedstaaten oder vom Europäischen Datenschutzbeauftragten eingerichtet werden. Auch die Durchführung erfolgt unter direkter behördlicher Aufsicht und Anleitung. Eine Haftungserleichterung für die Beteiligten von KI-Reallaboren ist nicht vorgesehen. Sie bleiben für Schäden, die infolge der Erprobung auftreten, verantwortlich. Im Rahmen der KI-Reallabore ergeben sich gewisse Freiräume im Hinblick auf die Nutzung von personenbezogenen Daten. Bislang war es so, dass bereits erhobene personenbezogene Daten nur in engen Grenzen nachgenutzt werden durften. Unter anderem musste sichergestellt sein, dass der Zweck der Nachnutzung mit dem ursprünglichen Erhebungszweck im engen Zusammenhang steht. Dies führte häufig dazu, dass eine Sekundärnutzung von personenbezogenen Daten, etwa zum Trainieren von KI-Modellen, ausgeschlossen war. Mit der KI-Verordnung soll nunmehr die Weiterverarbeitung von rechtmäßig erhobenen personenbezogenen Daten erleichtert werden. Der Anwendungsbereich für eine solche Weiterverarbeitung ist jedoch auf bestimmte Anwendungsbereiche beschränkt. Notwendig ist das Vorliegen eines erheblichen öffentlichen Interesses. Zu diesen privilegierten Einsatzbereichen zählen etwa die Strafverfolgung, die öffentliche Sicherheit und öffentliche Gesundheit, der Umweltschutz oder die Bereiche Energienachhaltigkeit, Transport und Mobilität.

1.7 Auswirkungen auf FuE-Projekte

Die KI-Verordnung enthält eine Vielzahl von Vorgaben, die zukünftig Einfluss auf die Entwicklung und den Einsatz von KI-Systemen haben werden. Rechtsunsicherheiten für Forschungsprojekte und Unternehmen ergeben sich vor allem im Hinblick auf die Frage, ob es sich bei der zu entwickelnden Software oder dem Produkt um ein KI-System handelt. Im Laufe des Legislativprozesses wurde der Begriff des KI-Systems mehrfach präzisiert und soll sich nunmehr nur auf Ansätze des maschinellen Lernens sowie logik- und wissensbasierte Ansätze beziehen. Software oder Produkte, die ohne diese Ansätze konzipiert sind, stellen damit kein KI-System dar und unterliegen damit auch nicht den Vorgaben der Verordnung. Anbieter und Nutzende von KI-Systemen mit einem geringen oder minimalen Risiko müssen aufgrund des risikobasierten Ansatzes zudem mit keinen bzw. nur sehr geringen Anforderungen rechnen. Anbieter von KI-Systemen mit einem geringen Risiko können sich auf Basis einer Selbstverpflichtung (Code of Conduct) zur Einhaltung von bestimmten Vorgaben festlegen.

In Bezug auf Hochrisiko-KI-Systeme ist eine Differenzierung vorzunehmen. KI-Systeme nach Anhang II Abschnitt B (KI-System ist Produkt oder Sicherheitskomponente eines Produkts und unterliegt einer EU-Sicherheitsregulierung, siehe Abschnitt 1.3.2, Fall 2) müssen die Vorgaben der Verordnung vorerst nicht unmittelbar beachten. Dennoch sollten Forschungsprojekte und Unternehmen, deren Produkte von den Rechtsakten nach Anhang II Abschnitt B betroffen sind, die Anforderungen der KI-Verordnung perspektivisch berücksichtigen. Denn die bereichsspezifischen Sicherheitsregulierungen werden durch die KI-Verordnung dergestalt angepasst, dass die Mindestanforderungen der Hochrisiko-KI-Systeme künftig im Rahmen der jeweiligen Rechtsakte berücksichtigt werden müssen.

Anbieter von KI-Systemen, die nach Anhang II Abschnitt A als hochriskant klassifiziert werden (siehe Abschnitt 1.3.2, Fall 1), müssen die Anforderungen der KI-Verordnung unmittelbar berücksichtigen. Bedenkt man, dass Produkte unter den dort aufgeführten Rechtsakten bereits jetzt einer strengen Sicherheitsüberprüfung unterliegen (z. B. bei der Entwicklung von Medizinprodukten), erweitert sich der Pflichtenkatalog für Anbieter solcher Systeme zusätzlich. Gleiches gilt für KI-Systeme, die in besonders sensiblen Bereichen (kritische Infrastruktur, Bildung, Beschäftigung etc.) eingesetzt werden und ein erhebliches Risiko für schützenswerte Rechtsgüter bergen (Anhang-III-Systeme, siehe Abschnitt 1.3.2, Fall 2).

Für Forschungsprojekte, aber auch für Akteure in Industriekooperationen kann die sehr schematische Einordnung in die Kategorien „Anbieter" und „Nutzer" zu Umsetzungsschwierigkeiten führen. Gerade große Forschungsprojekte mit einer Vielzahl von Kooperationspartnern sind durch eine arbeitsteilige Vorgehensweise geprägt. Häufig verteilt sich die Zuständigkeit für die Forschung an bzw. Entwicklung von KI-basierten Produkten oder Diensten über eine Vielzahl von Akteuren und Institutionen. Mit Blick auf die zu erfüllenden Compliance-Vorgaben muss Klarheit darüber bestehen, wer in welchem Umfang für die Umsetzung der Mindestanforderungen verantwortlich ist. Die in der KI-Verordnung vorgesehenen Sorgfaltspflichten setzen voraus, dass man bereits in einer frühen Projektphase die gesetzlichen Anforderungen mitdenkt. Insgesamt müssen die betroffenen Akteure zukünftig mit einem höheren Aufwand für ihre KI-Compliance rechnen. Dies gilt insbesondere vor dem Hintergrund, dass die Sorgfaltspflichten über den gesamten KI-Lebenszyklus eingehalten werden müssen.

Die Möglichkeit der Einrichtung von KI-Reallaboren kann positive Impulse auf das Innovationsgeschehen haben. Der Betätigungsbereich für FuE-Projekte ist jedoch insgesamt beschränkt. Die Bedingungen für den Betrieb der KI-Reallabore, einschließlich der Genehmigungskriterien, stehen derzeit nicht fest, sondern müssen im Rahmen von Durchführungsrechtsakten durch die EU-Kommission festgelegt werden. Zudem unterliegen die Einrichtung und Durchführung der KI-Reallabore einer strengen behördlichen Aufsicht. Forschungsprojekte sind in diesem Zusammenhang auf die enge Kooperation mit den Aufsichtsbehörden angewiesen.

1.8 Umsetzungsstand

Die KI-Verordnung wird voraussichtlich im dritten Quartal 2023 verabschiedet. Nach ihrer Annahme wird die Verordnung 20 Tage nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in Kraft treten. Nach einer Übergangszeit von 36 Monaten wird die Verordnung voraussichtlich 2026 unmittelbar und ohne weiteren nationalen Umsetzungsakt EU-weit anwendbar sein. Für KI-Systeme, die bereits vor diesem Zeitpunkt in Verkehr gebracht oder in Betrieb genommen wurden, greift ein Bestandsschutz. Für sie gilt die Verordnung nur, wenn die Systeme in ihrer Konzeption oder Zweckbestimmung in der Zwischenzeit wesentlich geändert werden.

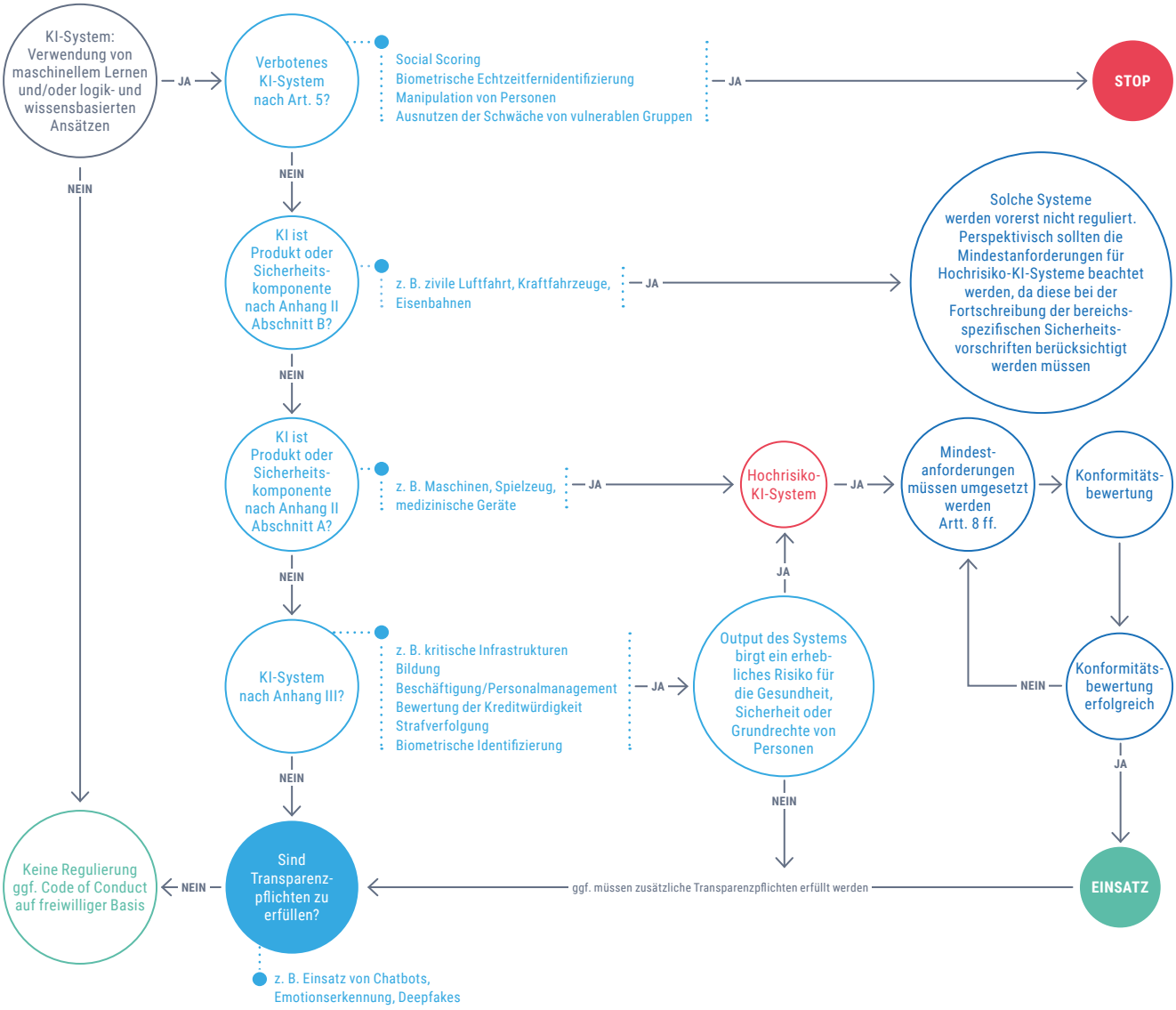


Abbildung 5: Das Prüfschema der KI-Verordnung

02

2 DATA GOVERNANCE ACT (DGA)

Im November 2020 hat die Europäische Kommission den Verordnungsentwurf über einen europäischen Data Governance Act (DGA) präsentiert. Im Zuge der Umsetzung der Datenstrategie[4] enthält der Rechtsakt Anforderungen für eine europäische Daten-Governance. Damit will die EU die Entwicklung eines grenzfreien digitalen Binnenmarktes sowie eine auf den Menschen ausgerichtete, vertrauenswürdige und sichere Datengesellschaft und -wirtschaft verwirklichen.

2.1 Anwendungsbereich und Adressatenkreis

Der DGA betrifft unterschiedliche Akteure und Anwendungsbereiche. Zunächst werden Regelungen für die Nutzung von besonders sensiblen Daten des öffentlichen Sektors festgelegt. Öffentliche Stellen wie Behörden, Kommunen sowie öffentliche Körperschaften usw. müssen künftig Vorgaben hinsichtlich der Bereitstellung von öffentlichen Datenbeständen einhalten. Daneben schafft der DGA einen Anmelde- und Aufsichtsrahmen für Datenvermittlungsdienste. Dabei handelt es sich um Dienste, wie Datenmarktplätze oder Ökosystemplattformen, die den Austausch zwischen Dateninhabern und Datennutzern organisieren. Bei den Vorgaben handelt es sich um horizontale Regelungen, die übergreifend in allen Sektoren und Branchen Anwendung finden. Schließlich soll durch den DGA die Etablierung von sogenannten datenaltruistischen Organisationen gefördert werden, die freiwillige „Datenspenden" zu Zwecken des Gemeinwohls organisieren. Datenaltruistische Organisationen zeichnen sich u. a. dadurch aus, dass sie die Datenverwaltung im Interesse des Dateninhabers und unabhängig von finanziellen (Eigen-)Interessen ausüben. Zur Steigerung der Vertrauenswürdigkeit werden Vorgaben für die staatliche Anerkennung und Eintragung von datenaltruistischen Organisationen in ein öffentliches Register geschaffen.

Abbildung 6: Anwendungsbereich und Adressatenkreis des Data Governance Acts

4 Siehe https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_de.

2.2 Bessere Verfügbarkeit von Daten öffentlicher Stellen

Die Erschließung von Datenbeständen des öffentlichen Sektors stellt ein Kernanliegen der europäischen Datenstrategie dar. Mit der Open-Data-Richtlinie[5] wurde bereits 2019 ein Rechtsrahmen geschaffen, der die Zugänglichkeit von Daten der öffentlichen Hand erleichtern soll. Die Vorgaben der Open-Data-Richtlinie wurden mit dem Datennutzungsgesetz (DNG) in nationales Recht überführt. Dort wird u. a. festgelegt, dass Daten im Besitz von öffentlichen Stellen (z. B. Behörden, Kommunen, Einrichtungen des öffentlichen Rechts) kommerziell oder nichtkommerziell nachgenutzt werden dürfen. Die Herausgabe von besonders sensiblen Daten war bislang nur eingeschränkt und nur unter Einhaltung von verfahrenstechnischen und rechtlichen Anforderungen möglich. Erschwerend kam hinzu, dass die Anforderungen an eine Nutzung dieser Daten in den einzelnen EU-Staaten sehr unterschiedlich geregelt waren. Mit dem DGA sollen nunmehr EU-weit einheitliche Bedingungen für die Weiterverwendung von sensiblen Daten der öffentlichen Hand gelten. Öffentliche Stellen sind angehalten, den Schutz von sensiblen Daten zu gewährleisten, etwa indem personenbezogene Daten anonymisiert oder Geschäftsgeheimnisse nur in aggregierter oder aufbereiteter Form weitergegeben werden dürfen. Zudem soll die Bereitstellung über eine „sichere Verarbeitungsumgebung" erfolgen. Zum Schutz des Wettbewerbs wird zudem ein Verbot von Ausschließlichkeitsvereinbarungen statuiert. Das bedeutet, dass die Vergabe von exklusiven (Datennutzungs-)Lizenzen unter Ausschluss weiterer Marktteilnehmer unzulässig ist. Der öffentlichen Stelle steht es jedoch frei, Datennutzungsgebühren zu erheben. Zugunsten von KMU, Start-ups und Bildungseinrichtungen darf die Gebühr ermäßigt werden. Die Bedingungen der Weiterverwendung können durch Nutzungsbedingungen festgelegt werden. Diese müssen transparent, nichtdiskriminierend, verhältnismäßig und objektiv gerechtfertigt sein und dürfen nicht zu Wettbewerbsbeschränkungen führen. Um den Prozess des Datenzugangs zu erleichtern, soll zudem eine zentrale Stelle eingerichtet werden, die die öffentliche Verwaltung bei der Umsetzung der Vorgaben unterstützt. Die Mitgliedstaaten können der zentralen Stelle zudem die Befugnis einräumen, selbst Datenzugangsentscheidungen zu treffen. Um diesen Aufgaben gerecht zu werden, soll die zentrale Stelle mit ausreichend finanziellen, technischen und personellen Mitteln ausgestattet sein. Um potenziellen Nutzenden dabei zu helfen, relevante Informationen darüber zu finden, welche Daten sich im Besitz der Behörden befinden, sollen die Mitgliedstaaten zudem eine zentrale nationale Informationsstelle einrichten.

Abschließend ist darauf hinzuweisen, dass durch die Regelungen des DGA keine neuen Zugangsrechte zu öffentlichen Datenbeständen geschaffen werden. Es werden lediglich die Rahmenbedingungen für die Bereitstellung von vorhandenen, bisher aber unerschlossenen Datenbeständen vereinheitlicht.

5 Richtlinie (EU) 2019/1024 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32019L1024.

2.3 Regulierung von Datenvermittlungsdiensten

Ein zentraler Bestandteil des DGA ist die Regulierung von Datenvermittlungsdiensten. Dabei handelt es sich um Anbieter, die als neutraler Intermediär zwischen Dateninhabern und Datennutzern vermitteln und damit deren gemeinsame Datennutzung ermöglichen. Datenvermittlungsdiensten ist die Monetarisierung dieser Daten nicht gestattet; sie dürfen die vermittelten Daten weder weiterverkaufen noch für die eigene Produktentwicklung nutzen. Datenvermittlungsdienste müssen vielmehr Neutralität gewährleisten und jedwede Interessenkonflikte vermeiden. Daher wird eine strenge strukturelle (und rechtliche) Trennung zwischen dem Datenvermittlungsdienst einerseits und allen anderen Dienstleistungen verlangt.

Datenvermittlungsdiensten wird eine Schlüsselrolle in der Datenwirtschaft zugeschrieben.[6] Ziel ist, durch die Etablierung von neutralen Datenmittlern das Vertrauen in die gemeinsame Nutzung von Daten zu stärken. Als Beispiele für Datenvermittlungsdienste nennt der DGA u. a. Datenmarktplätze oder Plattformen zur Organisation von Ökosystemen, die sich an eine Vielzahl von potenziellen Datennutzern richten.[7] Geschlossene Datenplattformen sollen demgegenüber nicht als Datenvermittlungsdienste gelten. Hierzu gehören Plattformen, in denen Unternehmen Daten in nichtöffentlichen Gruppen teilen, etwa im Rahmen von Lieferanten- und Kundenbeziehungen. Anbieter, die Daten lediglich aggregieren, anreichern oder umwandeln und hieraus eigene Datenprodukte erstellen und vermarkten, gelten ebenso wenig als Datenvermittlungsdienst, da hierbei keine unmittelbare Geschäftsbeziehung zwischen Dateninhabern und -nutzern hergestellt wird. Auch Cloud-Anbieter, Data-Sharing-Services oder Analysedienste fallen nicht in den Anwendungsbereich des DGA, sofern es sich nur um technische Werkzeuge zur gemeinsamen Datennutzung handelt, die nicht darauf abzielen, eine geschäftliche Beziehung zwischen Dateninhabern und -nutzern herzustellen.

DATENVERMITTLUNGSDIENST	**KEIN** DATENVERMITTLUNGSDIENST
Datenmarktplätze, die offen für alle Marktteilnehmer sind und den Handel mit Datenbeständen ermöglichen	Datenbroker, die Daten einer Vielzahl von Unternehmen ankaufen, um sie aufzubereiten und anschließend an andere Unternehmen weiterzuverkaufen (Datenveredlung)
„Datentreuhänder", die als vertrauenswürdige Instanz Datenzugangs- und Datennutzungsentscheidungen im Interesse des Dateninhabers ausüben	Geschlossene Datenplattformen, die beispielsweise Transaktionen zwischen einer begrenzten Anzahl von Lieferanten und Kunden abwickeln.
Orchestrierer von Ökosystemen, z. B. Plattformen, die den Austausch von Daten zwischen Akteursgruppen in einem bestimmten Wirtschaftsbereich organisieren	Rein technische Werkzeuge zur gemeinsamen Datennutzung wie Cloud-Speicher, Analysedienste, Software zur gemeinsamen Datennutzung, Internetbrowser oder Browser-Plug-ins, E-Mail-Dienste
Match-Making-Dienste, z. B. Dienste, die die Herstellung einer Geschäftsbeziehung nach zuvor festgelegten Kriterien ermöglichen	

Tabelle 1 Beispiele für Datenvermittlungsdienste sowie Dienste, bei denen es sich nicht um einen Datenvermittlungsdienst im Sinne des DGA handelt

6 Erwägungsgrund 27 des DGA.
7 Erwägungsgrund 28 des DGA.

PRAXISBEISPIEL

Ein Unternehmen bietet über eine Plattform digitale Karten und Geodatendienste an. Neben der Bereitstellung von eigenen Kartendaten (2D-Geodarstellung von Straßennetzen, Wegen, Gebäuden, Strukturen, Orten, Landnutzung, Bodenbedeckung usw.) sowie Zusatzdiensten (wie bspw. Routenplanung) werden auch Daten von Dritten, bspw. Verkehrsdaten von ÖPNV-Betreibern, über die Plattform angeboten. Geht man davon aus, dass die Daten von diesen Drittunternehmen unverändert nach einem Marktplatzprinzip verkauft werden, tritt das Unternehmen als Datenvermittlungsdienst im Sinne des DGA auf. Es wird daher künftig notwendig sein, die Bereiche Datenvermittlung und Angebot von datenbasierten Zusatzdiensten zu entflechten. Hierfür muss die Datenvermittlung durch eine eigenständige juristische Person erbracht werden. Zudem muss sich der Dienst vor Aufnahme seiner Tätigkeit registrieren und eine Vielzahl von regulatorischen Vorgaben erfüllen (siehe Abschnitt 2.3).

Anders liegt der Fall, wenn Datenbestände von Drittunternehmen aufgekauft wurden, um sie anschließend zu aggregieren und anzureichen. Ein Beispiel wäre der Aufkauf von Wareneins- und -ausgangsdaten verschiedener Einzelhandelsunternehmen, die anschließende Aggregation und Aufbereitung zu globalen Marktdaten, beispielsweise zur Analyse, wann (bspw. saisonal oder anderweitig zyklisch bedingt), wie oft und welche Produkte im Einzelhandel ge- und verkauft werden. Der Verkauf von derartig veredelten Datenbeständen stellt keine Datenvermittlung dar (siehe Tabelle 1). Die gesetzlichen Anforderungen an Datenvermittlungsdienste müssten dann nicht umgesetzt werden.

Der DGA enthält einen umfassenden Anforderungskatalog für Datenvermittlungsdienste. Die Einhaltung der Anforderung wird behördlich überwacht und Verstöße können mit Bußgeldern geahndet werden. Zur besseren Erfassung von Anbietern innerhalb der EU müssen sich diese vor Aufnahme ihrer Tätigkeit behördlich registrieren. Sobald die Anmeldung erfolgt ist, darf die Tätigkeit aufgenommen werden. Dabei muss eine Reihe von Vorgaben eingehalten werden. Im Mittelpunkt steht das Neutralitätsgebot. Es sieht eine strenge Trennung zwischen Datenvermittlung und Datennutzung vor. Der Anbieter darf danach nur als Mittler tätig sein und die Daten für keine anderen Zwecke verwenden. Untersagt wären demnach etwa datenbezogene Produkte oder Dienste wie etwa KI-basierte Datenanalysen oder -services.

Erlaubt sind lediglich Metadatenanalysen, wenn sie der Verbesserung des Datenvermittlungsdienstes dienen, etwa Maßnahmen zur Betrugsprävention oder zur Gewährleistung der Cybersicherheit. Ein zulässiges Betätigungsfeld sind zudem datenbezogene Angebote und Werkzeuge, die darauf ausgerichtet sind, den Datenaustausch zu erleichtern. Hierzu gehören Dienste zur Speicherung, Pflege, Konvertierung, Anonymisierung und Pseudonymisierung von Daten. Diese datenbezogenen Dienste dürfen jedoch nur mit Zustimmung des Dateninhabers verwendet werden. Der Datenvermittlungsdienst ist darüber hinaus verpflichtet, die ihm übergebenen Daten unverändert weiterzuleiten. Eine Umwandlung in andere Formate ist nur erlaubt, wenn dies der Verbesserung der Interoperabilität dient oder der Dateninhaber dies verlangt. Gleiches gilt, wenn eine Konvertierung in bestimmten Sektoren gesetzlich vorgeschrieben ist. Der Dateninhaber muss die Möglichkeit erhalten, der Konvertierung zu widersprechen („opt-out“).

Um die Neutralitätsvorgaben auch in der organisatorischen Struktur des Anbieters zu verankern, wird zudem vorgegeben, dass Datenvermittlungsdienste über eine gesonderte juristische Person bereitzustellen sind. Eine wichtige Anforderung zur Stärkung der Wahlfreiheit von Dateninhaber und Datennutzer ist die Vorgabe, dass die Inanspruchnahme des Vermittlungsdienstes nicht davon abhängig gemacht werden darf, dass weitere Dienstleistungen des Unternehmens in Anspruch genommen werden. Es wäre beispielsweise unzulässig, Preisnachlässe oder günstigere Konditionen nur zu gewähren, wenn Zusatzdienste eines Schwesterunternehmens gebucht werden (Hennemann und v. Ditfurth 2022, S. 1909). Als Ausdruck des Neutralitätsgedankens soll hinsichtlich des Zugangsverfahrens sichergestellt sein, dass dieses fair, transparent und nichtdiskriminierend ist. Es wäre demnach etwa unzulässig, bestimmte Akteure ohne sachlichen Grund auszuschließen. Das Diskriminierungsverbot umfasst auch die Preisbildung. Hierdurch soll eine Benachteiligung über die Preisfestsetzung ausgeschlossen werden. Gleichzeitig gebietet die Anforderung der Transparenz, dass die Zugangsbedingungen klar und verständlich kommuniziert werden müssen.

ERLAUBT	VERBOTEN
Verarbeitung, um Daten den Nutzenden zur Verfügung zu stellen	Nutzung der Daten außerhalb der Vermittlungstätigkeit für eigene Zwecke, etwa Angebot von datenbasierten Produkten oder Services wie Big-Data- oder KI-Analysen
Metadatenanalyse, sofern diese der Verbesserung des Vermittlungsdienstes dient, z. B. Maßnahmen zur Betrugsprävention oder zur Gewährleistung der Cybersicherheit	Bedingungen, die die Datennutzer dazu veranlassen, weitere kommerzielle Dienste des Anbieters wählen zu müssen
Umwandlung in andere Formate, wenn zur Herstellung von Interoperabilität zwischen den Sektoren notwendig oder wenn der oder die Nutzende dies wünscht oder die Umwandlung gesetzlich vorgeschrieben ist	Zugangsbedingungen inklusive Preise, die unfair, intransparent oder diskriminierend sind
Vorübergehende Speicherung, Pflege, Konvertierung, Anonymisierung und Pseudonymisierung von Daten, wenn vom Dateninhaber ausdrücklich gewünscht	

Tabelle 2 Übersicht zu den Bedingungen für die Erbringung von Datenvermittlungsdiensten

2.4 Datenaltruistische Organisationen

Bestimmte Datenquellen sind von hohem gesellschaftlichem Interesse. Um deren Potenziale besser nutzen zu können, bedarf es ausreichender Datenmengen. Mit dem DGA sollen die Voraussetzungen für die Entstehung ausreichender Datenmengen geschaffen werden. Dies soll u. a. auf Grundlage von Datenaltruismus geschehen. Hierunter wird die freiwillige gemeinsame Nutzung von Daten verstanden, die der Dateninhaber ohne Erhalt einer Gegenleistung (altruistisch) bereitstellt, um hiermit Ziele von allgemeinem Interesse zu fördern. Als solche gemeinwohlorientierten Ziele gelten die Gesundheitsversorgung, die Bekämpfung des Klimawandels, die Verbesserung der Mobilität oder die wissenschaftliche Forschung. Der DGA soll die Entstehung von datenaltruistischen Organisationen erleichtern. Beispielsweise sollen sie sich – sofern sie eine eigene Rechtspersönlichkeit aufweisen und Ziele von allgemeinem Interesse verfolgen – in ein öffentliches Register eintragen lassen können (siehe oben). Zur Wahrung ihrer Unabhängigkeit dürfen sie

zudem keinen Erwerbszweck verfolgen und müssen sicherstellen, dass die altruistische Tätigkeit von anderen Tätigkeiten strukturell getrennt ist. Zudem müssen datenaltruistische Einrichtungen bestimmte Transparenzanforderungen erfüllen und Vorgaben zur Wahrung der Rechte der Dateninhaber umsetzen. Die Einhaltung der Anforderungen wird behördlich überwacht. Um die Erhebung, insbesondere personenbezogener Daten, zu erleichtern, soll die Europäische Kommission einen Vorschlag für ein europäisches Einwilligungsformular ausarbeiten. Dieses soll modular aufgebaut sein, damit es für bestimmte Sektoren und Zwecke angepasst werden kann. Damit datenaltruistische Organisationen ohne Weiteres erkannt werden können, soll zudem ein in der gesamten EU wiedererkennbares Logo eingeführt werden. Das gemeinsame Logo soll zusammen mit einem QR-Code mit Link zum öffentlichen Unionsregister anerkannter datenaltruistischer Organisationen erscheinen.

2.5 Durchsetzung und Sanktionen

Zur Durchsetzung der Vorgaben des DGA sollen die Mitgliedstaaten Vorschriften über Sanktionen erlassen. Gegen Datenvermittlungsdienste oder datenaltruistische Organisationen, die künftig gegen die Bedingungen des DGA verstoßen, können demnach behördliche Maßnahmen getroffen werden. Wie und in welchem Umfang eine Sanktionierung erfolgen soll, wird nicht festgelegt. Geregelt wird lediglich, dass die Maßnahmen wirksam, verhältnismäßig und abschreckend sein sollen. Denkbar ist demnach etwa die Verhängung von Bußgeldern, wobei der DGA – anders als bei den anderen Rechtsakten – keinen konkreten Bußgeldrahmen vorgibt.

2.6 Auswirkungen auf FuE-Projekte

Mit den Regelungen zur Weiterverwendung von sensiblen Daten im Besitz öffentlicher Stellen werden die Rahmenbedingungen für die Verfügbarkeit von Open Data verbessert. Zugleich werden jedoch keine neuen Zugangsrechte geschaffen, sondern lediglich die Voraussetzungen vereinheitlicht, unter denen eine Weiterverwendung stattfinden kann. Inwieweit hierdurch die Dichte an verwertbaren Datenbeständen zunimmt, lässt sich derzeit noch nicht absehen. Dennoch sind die Neuregelungen aus der Perspektive von Forschungsprojekten, aber auch Unternehmen und Start-ups, als positiv zu bewerten. Denn nunmehr gelten EU-weit einheitliche Standards und Verfahren zur Erschließung von besonders sensiblen Daten der öffentlichen Hand. Außerdem kann die im DGA vorgesehene zentrale Informationsstelle dazu beitragen, dass der Antragsprozess vereinfacht wird. Die zu erstellende zentrale Bestandsliste kann zudem dafür sorgen, dass Daten leichter aufgefunden werden können. Praktische Probleme, insbesondere aufseiten der bereitstellenden Institutionen bleiben jedoch ungelöst: Etwa die Frage, wann Daten als anonymisiert gelten oder wann Gebühren für die Datenbereitstellung verhältnismäßig sind. Die datenwirtschaftlichen Impulse könnten in der Praxis hinter den Erwartungen zurückbleiben, weil die öffentliche Hand mit der Umsetzung der Vorgaben überfordert sein könnte.

Mit dem DGA wird darüber hinaus ein verbindliches Leitbild für die künftige Governance von Datenintermediären vorgegeben. Dieses gesetzlich angeordnete Framework wird erhebliche Auswirkungen auf die Ausgestaltung und Organisationsform von Datenintermediären haben. Betroffen sind vorrangig offene Plattformen wie Datenmarktplätze, Datendrehscheiben oder Datenplattformen für spezifische Branchenökosysteme. Die Neutralitätsvorgabe des DGA bewirkt, dass derartige Anbieter die über die Plattform vermittelten Daten nicht monetarisieren dürfen. Bestehende Anbieter von Datenvermittlungsdiensten müssen folglich ihr Geschäfts- und Betriebsmodell anpassen und gewährleisten, dass Datenvermittlungs- und Datennutzungsdienste strukturell voneinander getrennt werden. Dies erfordert u. a., dass der Datenvermittlungsdienst durch eine gesonderte juristische Person bereitgestellt wird. Forschungs- und Entwicklungsprojekte müssen bereits in einer frühen Projektphase ein Verständnis von der Rollenverteilung der jeweiligen Akteure innerhalb des Datenökosystems entwickeln. Dabei ist sicherzustellen, dass datenbasierte Zusatzdienste, wie KI- oder Big-Data-Analysen, nicht durch die Vermittlungsplattform selbst angeboten werden dürfen. Die Umsetzung der gesetzlichen Anforderungen bedeutet für Forschungsprojekte einen höheren Aufwand. In Bezug auf die Verwertungsphase ist zudem zu berücksichtigen, dass die reine Vermittlung von Daten den Spielraum für tragfähige Geschäftsmodelle stark beschränken kann. Diesen Einschränkungen stehen jedoch unter Umständen auch Vorteile gegenüber. Die Etablierung von neutralen Vermittlungsinstanzen kann auch zu einem höheren Vertrauen zwischen den Akteuren der Datenwirtschaft führen. Ob die vom Verordnungsgeber intendierte Etablierung von Datenvermittlungsdiensten tatsächlich eintritt, lässt sich derzeit nicht absehen.

Abbildung 7: Auswirkungen des DGA auf Datenintermediäre

Zukünftig könnte die Begünstigung von datenaltruistischen Organisationen zur Erschließung neuer Datenbestände führen. Profitieren könnten nichtkommerzielle Datenplattformen, die Ziele im allgemeinen gesellschaftlichen Interesse verfolgen. Auch für staatliche Institutionen bietet sich das im DGA angelegte Framework gegebenenfalls an. Durch die Bereitstellung eines einheitlichen Einwilligungsformulars könnten Unsicherheiten im Hinblick auf die Wirksamkeit einer Einwilligung abgebaut werden. Inwieweit der Ansatz zur Förderung von Datenaltruismus trägt und inwieweit hierdurch das Vertrauen zur Bereitstellung von Daten erhöht wird, lässt sich derzeit jedoch nicht abschätzen.

2.7 Umsetzungsstand

Der Data Governance Act ist bereits verabschiedet und wurde am 03.06.2022 im Europäischen Amtsblatt veröffentlicht. Die Verordnung ist ab dem 24. September 2023 unmittelbar in der gesamten EU anwendbar. Für Anbieter, die bereits am 23.06.2022 Datenvermittlungsdienste erbracht haben, gilt eine Übergangsfrist. Sie müssen den Verpflichtungen aus der Verordnung erst ab dem 24.09.2025 nachkommen.

03

3 DATA ACT (DA)

Als zweite Säule der europäischen Datenstrategie wird mit der Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung[8] (Data Act) ein weiteres datenwirtschaftliches Regulierungsvorhaben auf den Weg gebracht. Der Data Act schafft einen sektorenübergreifenden Governance-Rahmen für die gemeinsame Datennutzung und soll künftig festlegen, wer – außer dem Hersteller von Produkten – unter welchen Bedingungen und auf welcher Grundlage berechtigt ist, auf Daten zuzugreifen. Dem Legislativvorschlag liegt die Annahme zugrunde, dass ein Großteil der in Maschinen und Produkten enthaltenen Daten wirtschaftlich nicht verwertet werden können, da es an entsprechenden Zugriffsmöglichkeiten und -rechten fehlt.[9] Der Data Act soll bestehende Hindernisse für die gemeinsame Datennutzung zugunsten von Unternehmen, Verbraucherinnen und Verbrauchern sowie der öffentlichen Hand abbauen und neue Impulse für datengesteuerte Innovationen setzen.

3.1 Anwendungsbereich

Der Data Act adressiert vorrangig Hersteller, die ihre Produkte in der EU in den Verkehr bringen. Bei den Produkten muss es sich um Erzeugnisse handeln, die während ihrer Verwendung Daten über ihre Nutzung oder Umgebung generieren und die in der Lage sind, diese elektronisch zu übermitteln. Dies sind typischerweise vernetzte Produkte wie Maschinen, Fahrzeuge, Haushaltsgeräte oder elektronische Konsumgüter. Neben den Herstellern fallen auch Anbieter von sogenannten verbundenen Diensten in den Anwendungsbereich der Verordnung. Hierzu gehören digitale Dienste, die integraler Bestandteil eines Produkts sind und ohne die das Produkt nicht funktionieren würde. Der Data Act sieht vor, dass Hersteller von vernetzten (smarten, datenbasierten) Produkten diese künftig zugänglich gestalten müssen. Da sie die technisch-faktische Hoheit über die generierten Daten haben, unterliegen sie zudem als sogenannte Dateninhaber weiteren Verpflichtungen. Hierzu gehört die Pflicht, den Nutzenden des Produkts Zugang zu ihren Daten zu gewähren. Darüber hinaus besteht die Verpflichtung, auf Verlangen der Nutzenden auch Dritten Zugang zu den Daten zu gewähren. Bei diesen Datenempfängern handelt es sich um Akteure, die im Auftrag der Nutzenden tätig werden und denen Daten im Rahmen einer gewerblichen, geschäftlichen, handwerklichen oder beruflichen Tätigkeit bereitgestellt werden. Kategorien von Datenempfängern sind beispielsweise Anbieter von datenbasierten Dienstleistungen oder auch Anbieter im Aftermarket-Bereich wie Autowerkstätten oder Wartungsdienste.

8 https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52022PC0068&from=EN.
9 Eine Ausnahme gilt für personenbezogene Daten, wenn betroffene Personen nach den Vorschriften der EU-Datenschutz-Grundverordnung ein Recht auf Auskunft und Datenportabilität haben.

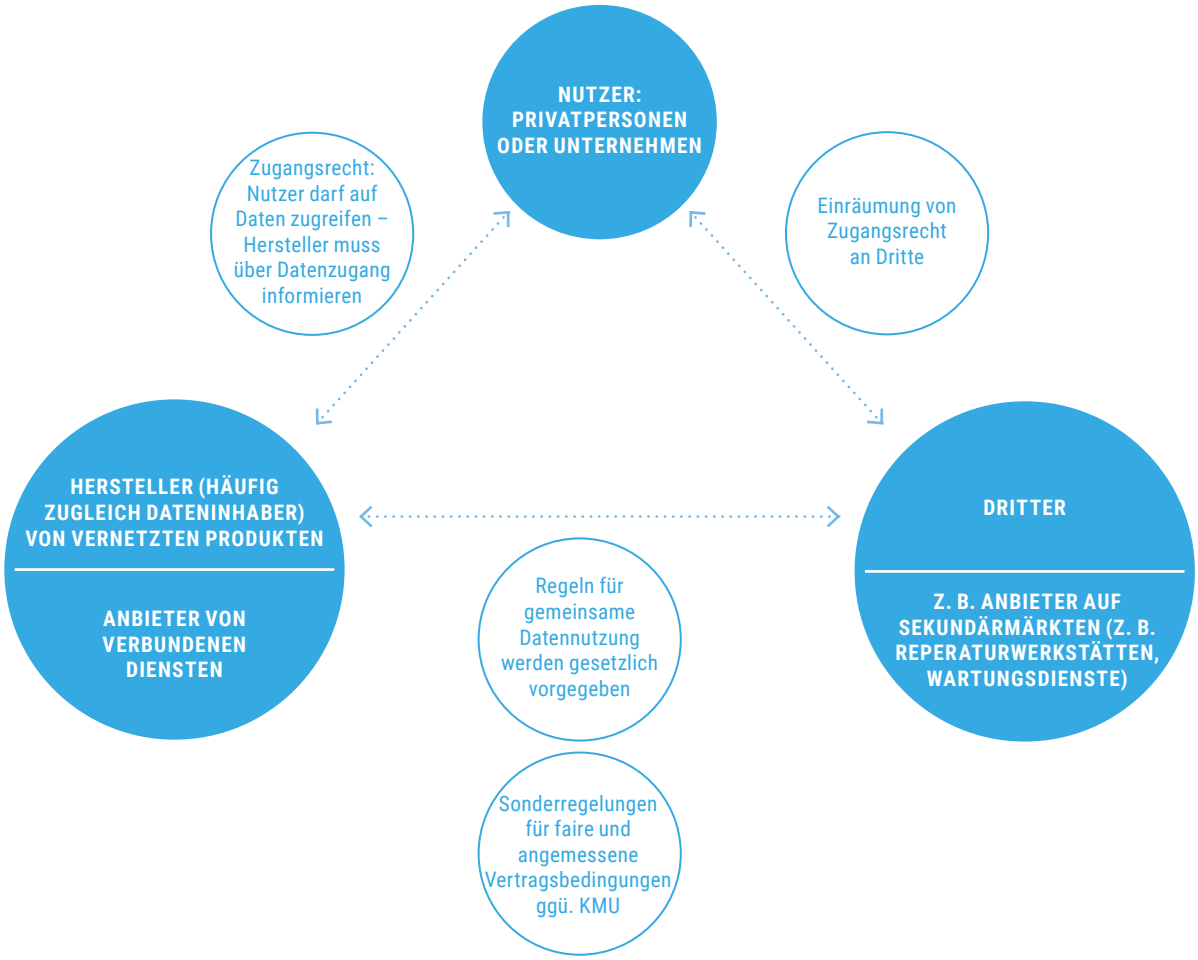


Abbildung 8: Übersicht zu den Beziehungen und Ansprüchen der Akteure

3.2 Pflicht zur Zugänglichmachung von Nutzungsdaten

Der Data Act formuliert zunächst Pflichten im Hinblick auf die Produktgestaltung. Wertschöpfung auf Grundlage von Daten erfordert zunächst, dass diese auch technisch verfügbar sind. Künftig besteht die Pflicht, Produkte so zu konzipieren und herzustellen, dass die bei ihrer Nutzung erzeugten Daten standardmäßig für die Nutzenden einfach, sicher und direkt zugänglich sind (Accessibility by Default). Um die potenziellen Möglichkeiten der Datenverwertung erkennbar zu machen, soll der Hersteller künftig zudem verpflichtet sein, bestimmte Transparenz- und Informationspflichten gegenüber dem Käufer, Mieter oder Leasingnehmer eines Produkts zu erfüllen. Hierzu gehört etwa die Offenlegung über die Art und den Umfang der durch die Nutzung entstehenden Daten und wie die Nutzenden auf diese Daten zugreifen können.

3.3 Recht der Nutzenden auf Datenzugang

Damit Nutzende auf die von ihnen generierten Daten zugreifen können, werden auch hier – über die Vorgaben zur Produktgestaltung hinaus – die rechtlichen Rahmenbedingungen geschaffen: das Recht auf Datenzugang. Dieses Recht besteht gegenüber dem Dateninhaber, also demjenigen, der durch die Kontrolle über die technische Konzeption des Produktes in der Lage ist, bestimmte Daten bereitzustellen. Auf Verlangen der Nutzenden muss der Dateninhaber (in der Regel der Hersteller) die bei der Nutzung eines Produktes erzeugten Daten unverzüglich, kostenlos und gegebenenfalls kontinuierlich und in Echtzeit zur Verfügung stellen. Kleinst- oder Kleinunternehmen[10] sind von der Pflicht zur Datenbereitstellung befreit. Um die Interessen des Dateninhabers zu schützen, sind Beschränkungen des Datenzugangsrechts vorgesehen. So müssen Geschäftsgeheimnisse des Dateninhabers nur offengelegt werden, wenn alle notwendigen Maßnahmen getroffen worden sind, um die Vertraulichkeit der Geschäftsgeheimnisse, insbesondere gegenüber Dritten, zu wahren. Der Verordnungsgeber zielt dabei offenbar auf den Abschluss von Vertraulichkeitsvereinbarungen ab (Hennemann und Steinrötter 2022, S. 1484). Als weitere Beschränkung ist es den Nutzenden untersagt, mit den erlangten Daten selbst Produkte zu entwickeln, die im Wettbewerb mit den Produkten des Dateninhabers stehen. Eine weitere datenrechtliche Neuerung ist der Umstand, dass der Dateninhaber (z. B. der Hersteller einer Maschine) die während der Nutzung entstehenden Daten nicht ohne Weiteres für eigene Zwecke verwenden darf. Eine Verarbeitung der Daten ist nur zulässig, wenn es eine entsprechende vertragliche Vereinbarung zwischen Dateninhaber und -nutzer gibt. Dies macht es erforderlich, dass eine Zustimmung zur Datennutzung von dem bzw. der Nutzenden eingeholt werden muss, beispielsweise wenn die Daten zur Weiterentwicklung der eigenen Produkte verwendet werden sollen.

Das Zugangsrecht bezieht sich auf alle Daten, die durch die Nutzung des Produkts entstehen. Dies umfasst auch absichtlich durch die Nutzenden generierte Daten sowie Daten, die als Nebenprodukt von Nutzeraktionen erzeugt werden (z. B. Diagnosedaten). Erfasst werden aber auch Daten, die ohne jegliche Nutzerinteraktion entstehen, etwa, wenn sich das Produkt im Bereitschaftszustand befindet oder ausgeschaltet ist.[11] Mit umfasst sind auch Umgebungsdaten, die infolge der Benutzung entstehen (z. B. Daten zur Raumtemperatur). Nicht zugänglich sind hingegen abgeleitete Daten, also Informationen, die erst durch eine Analyse der Nutzungsdaten durch den Dateninhaber entstehen.

3.4 Recht auf Weitergabe von Daten an Dritte

Auf Verlangen der Nutzenden muss der Dateninhaber die bei der Nutzung eines Produktes erzeugten Daten auch einem Dritten bereitstellen, wobei die gleichen Anforderungen gelten wie bei der Datenbereitstellung an die Nutzenden selbst. Die Verfügbarmachung muss insbesondere unverzüglich und für die Nutzenden kostenlos erfolgen. Beschränkungen bestehen gegenüber großen Plattformdiensten. Diese sind keine zulässigen Datenempfänger, sofern sie aufgrund ihrer Marktstellung als Gatekeeper im Sinne des Digital Markets Act benannt wurden (siehe folgendes Kapitel 5). Die Bereitstellung an diese Dienste kann folglich durch den Dateninhaber verweigert werden.

10 Nach Art. 2 der Empfehlung 2003/361/EG sind Kleinstunternehmen Unternehmen mit weniger als zehn Mitarbeiterinnen und Mitarbeitern und einem Jahresumsatz oder einer Jahresbilanzsumme von höchstens zwei Millionen Euro. Kleine Unternehmen sind Unternehmen, die weniger als 50 Mitarbeitende und einen Jahresumsatz oder eine Jahresbilanzsumme von höchstens zehn Millionen Euro haben. Mittlere Unternehmen sind Unternehmen, die weniger als 250 Mitarbeitende und einen Jahresumsatz von höchstens 50 Millionen Euro oder eine Jahresbilanzsumme von höchstens 43 Millionen Euro haben.

11 Erwägungsgrund 17 des Data Act.

Der Dateninhaber kann das Weitergabeverlangen der Nutzenden nicht pauschal mit Verweis auf den Geschäftsgeheimnisschutz ablehnen. Geschäftsgeheimnisse müssen Dritten aber nur insoweit offengelegt werden, als dies für den zwischen dem bzw. der Nutzenden und dem Dritten vereinbarten Zweck unbedingt erforderlich ist und der Dritte alle zwischen ihm und dem Dateninhaber vereinbarten besonderen Maßnahmen getroffen hat, die erforderlich sind, um die Vertraulichkeit des Geschäftsgeheimnisses zu wahren. Die Eigenschaft als Geschäftsgeheimnis und Maßnahmen zur Wahrung der Vertraulichkeit sollen zwischen Dateninhaber und Dritten (vertraglich) festgelegt werden.

Der Datenempfänger darf die ihm übertragenen Daten seinerseits nicht nach Belieben verwenden. Zum Schutz des Dateninhabers ist es ihm etwa untersagt, die erhaltenen Daten für die Entwicklung von Konkurrenzprodukten zu verwenden oder diese an zentrale Plattformdienste weiterzuleiten (Gatekeeper im Sinne des Digital Markets Act). Zur Wahrung der Interessen der Nutzenden ist es dem Dateninhaber zudem untersagt, die erhaltenen Daten für Zwecke des Profilings zu nutzen.

3.5 Bedingungen der Datenbereitstellung

Der Data Act eröffnet nicht nur die Möglichkeit der Datennutzung durch Dritte. Er regelt auch die Rahmenbedingungen, unter denen die Daten zugänglich gemacht werden sollen. Eine zentrale Bestimmung betrifft dabei die Vertragsbedingungen zwischen Dateninhaber und -empfänger. Diese müssen den FRAND-Bedingungen entsprechen, also fair, angemessen und nichtdiskriminierend sein. Für die Bereitstellung der Daten darf der Dateninhaber vom Datenempfänger eine Gegenleistung, etwa in Form einer Vergütung, fordern. Diese muss jedoch angemessen sein. Zudem sind Vorgaben in Bezug auf technische Schutzmaßnahmen zulässig. Vorgesehen ist außerdem die Einrichtung von Streitbeilegungsstellen, die u. a. die Aufgabe haben, die Vertragsbedingungen im Hinblick auf ihre Fairness, Angemessenheit und Diskriminierungsfreiheit zu überprüfen.

3.6 Regelungen zum Schutz von KMU

Der Data Act enthält an verschiedenen Stellen Vorschriften zum Schutz von schwächeren Marktteilnehmern. So werden etwa Klein- und Kleinstunternehmen als Dateninhaber von den oben genannten Pflichten zur Datenbereitstellung befreit. Handelt es sich bei einem Datenempfänger um ein Klein- oder Kleinstunternehmen, greifen zudem Vorschriften zur Verhinderung von missbräuchlichen Klauseln in Bezug auf Datenzugang und Datennutzung. Hierdurch soll durch Einschränkung der Vertragsfreiheit gewährleistet werden, dass auch schwächere Vertragsparteien zu fairen Bedingungen an der datenbasierten Wertschöpfung partizipieren können. Adressiert werden dabei Vertragsbedingungen, die einem Kleinstunternehmen, einem kleinen oder mittleren Unternehmen einseitig von einer Vertragspartei auferlegt werden. Sind diese Vertragsbedingungen missbräuchlich, sind sie für die benachteiligte Vertragspartei nicht bindend. In Bezug auf die Missbräuchlichkeit einer Vertragsklausel kommt es darauf an, ob diese von der guten Geschäftspraxis abweicht und gegen das Gebot von Treu und Glauben und des redlichen Geschäftsverkehrs verstößt. Vertragsbedingungen in Bezug auf den Datenzugang und die Datennutzung unterliegen damit einer Inhaltskontrolle, vergleichbar mit der AGB-Klauselkontrolle in den Vorschriften des

BGB (Klink-Straub und Straub 2022). Auch hinsichtlich der Vergütung, die der Dateninhaber für die Bereitstellung von Daten an Dritte vorsehen kann, werden Klein- und Kleinstunternehmen privilegiert. Zulässig sind Kosten, die nicht höher sein dürfen als die Kosten, die mit der Bereitstellung der Daten für den Datenempfänger unmittelbar zusammenhängen.

3.7 Wechsel zwischen Cloud-Anbietern

Der Data Act enthält zudem Regelungen, die darauf abzielen, den Wechsel zwischen Cloud-Anbietern zu erleichtern. Konkret sollen gewerbliche, technische, vertragliche und organisatorische Hürden abgebaut werden, die einen Wechsel erschweren oder verhindern. Vorgesehen sind etwa Vorgaben hinsichtlich der vertraglichen Rahmenbedingungen wie eine maximale Kündigungsfrist von 30 Tagen oder die Möglichkeit, Daten von einem Anbieter zu einem anderen Anbieter übertragen zu können. Hierbei müssen die Anbieter von Cloud-Services den Kunden beim Wechselvorgang unterstützen und die uneingeschränkte Kontinuität bei der Erbringung der jeweiligen Funktionen oder Dienste sicherstellen. In diesem Zusammenhang sollen auch Entgelte für einen beantragten Wechsel entfallen bzw. für bestimmte Transaktionen auf die Grenzkosten beschränkt werden. Daneben werden technische Vorgaben hinsichtlich der Verwendung von offenen Schnittstellen sowie die Kompatibilität mit offenen Interoperabilitätsspezifikationen oder europäischen Interoperabilitätsnormen eingefordert.

3.8 Datenbereitstellung an öffentliche Stellen

Darüber hinaus ist auch eine Datenbereitstellungspflicht zugunsten von öffentlichen Stellen oder Einrichtungen der EU vorgesehen. Dies ist allerdings nur in außergewöhnlichen Notstandslagen möglich und zudem zeitlich befristet. Qualitativ muss die Notstandslage so gravierend sein, dass mit schwerwiegenden und dauerhaften Folgen für die Lebensbedingungen oder die wirtschaftliche Stabilität zu rechnen ist. Das Herausverlangen von Daten durch öffentliche Stellen ist nur zulässig, wenn die Daten zur Bewältigung eines öffentlichen Notstands tatsächlich erforderlich sind und dem Staat auch keine anderen Datenquellen zur Verfügung stehen. Im Falle eines öffentlichen Notstands sind staatliche Institutionen zudem befugt, die erhaltenen Daten an Forschungsorganisationen weiterzugeben. Berechtigt sind jedoch nur gemeinnützige Organisationen oder solche, die im öffentlichen Interesse handeln. Die Forschungseinrichtungen dürfen zudem nicht unter dem bestimmenden Einfluss von gewerblichen Unternehmen stehen.

3.9 Durchsetzung und Sanktionen

Die Aufsicht und Durchsetzung der Vorgaben der Verordnung erfolgt auf nationaler Ebene. Jeder Mitgliedstaat benennt hierzu eine oder mehrere zuständige Behörden, die u. a. die Aufgabe haben, über Inhalt und Pflichten der Verordnung aufzuklären. Die zuständige Behörde bearbeitet zudem Beschwerden in Bezug auf mögliche Verstöße und ist zur Verhängung von Sanktionen berechtigt, was auch Zwangsgelder und Geldstrafen umfassen kann. Die Sanktionen müssen dabei wirksam, verhältnismäßig und abschreckend sein. Dabei sind Geldbußen in Höhe von bis zu 20 Millionen Euro oder vier Prozent des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs möglich.

3.10 Auswirkungen auf FuE-Projekte

Der Data Act basiert auf einem horizontalen Regulierungsansatz. Das bedeutet, er legt Regeln für eine gemeinsame Datennutzung fest, die sektorenübergreifend und unabhängig von einer bestimmten Branche gelten. Die Bewertung der Auswirkungen des Rechtsakts sind vorläufig, da sich der Data Act noch mitten im Gesetzgebungsverfahren befindet (Stand Dezember 2022). Es ist zu erwarten, dass es im weiteren Legislativprozess zu umfangreichen Änderungen am Verordnungstext kommen wird.

Der Rechtsakt hat zunächst Auswirkungen auf Forschungsprojekte und Unternehmen, die auf die Entwicklung von vernetzten Produkten ausgerichtet sind. Bereits in der Entwicklungsphase eines Produkts muss darauf geachtet werden, dass die entstehenden Nutzungsdaten standardmäßig, einfach, sicher und direkt zugänglich sind. Gleiches gilt für die Gestaltung von verbundenen Diensten, also solchen, die mit vernetzten Produkten interagieren und fester Bestandteil von diesen sind. Plattformen, Schnittstellen oder Benutzeroberflächen müssen dementsprechend auch den Grundsatz „Accessibility by Default" umsetzen. In Forschungsprojekten bedarf es hierfür einer engen Abstimmung zwischen den Akteuren. Dies betrifft sowohl die Entwicklung des physischen Produkts selbst, als auch die darauf aufsetzende Software. Darüber hinaus muss, nicht zuletzt im Hinblick auf die zu erfüllenden Informationspflichten, Klarheit darüber herrschen, welche Daten als „Nutzungsdaten" der Bereitstellungspflicht unterliegen. Zudem müssen Vorkehrungen getroffen werden, wie die Nutzenden über die ihnen bereitstehenden Daten und Rechte informiert werden sollen. Schließlich sollte auch beachtet werden, dass der Hersteller die generierten Nutzungsdaten für eigene Zwecke nur dann verwenden darf, wenn er zuvor die Zustimmung des bzw. der Nutzenden eingeholt hat.

Die im Data Act angelegten Akteursbeziehungen (Dateninhaber, Nutzer und Datenempfänger) können bei Forschungs- und Entwicklungsprojekten zu Umsetzungsschwierigkeiten führen. Eine derart vereinfachte Dreiecksbeziehung wird der in FuE-Projekten bestehenden Aufgaben- und Arbeitsteilung, insbesondere in komplexen Datenökosystemen, häufig nicht gerecht werden. Die Akteure in Forschungsprojekten, aber auch in Industriekooperationen müssen sich künftig stärker dahingehend abstimmen, wer die jeweiligen Rollen und die damit verbundenen Verantwortlichkeiten innehat. Zudem wird im Data Act der Schutz von Geschäftsgeheimnissen der Dateninhaber nicht als vorrangiges Ziel gesehen, sondern gegenüber den Interessen der anderen Akteure abgewogen. Insbesondere dürfen Zugangsbegehren nicht pauschal mit Verweis auf die Sensibilität von Unternehmensdaten abgelehnt werden. Damit wird in FuE-Projekten, aber auch im unternehmerischen Kontext, künftig ein stärkeres Augenmerk auf die technischen und rechtlichen Schutzvorkehrungen gelegt, die den Datenempfängern zur Wahrung der Vertraulichkeit der bereitgestellten Daten auferlegt werden.

Forschungsprojekte und Unternehmen müssen dafür Sorge tragen, dass die Produkte so gestaltet werden, dass Nutzende das Recht auf Datenzugang wirksam ausüben können. Anfallende Nutzungsdaten müssen auf Anfrage unverzüglich und gegebenenfalls kontinuierlich und in Echtzeit zur Verfügung gestellt werden. Gleiches gilt im Hinblick auf die Weitergabe von Daten an Dritte. Auch hier muss sichergestellt werden, dass Anfragen der Nutzenden umgehend erfüllt werden können. In Bezug auf die Weitergabe von Daten an Dritte müssen künftig die Umstände der Datenüberlassung zwischen Dateninhaber und Datenempfänger festgelegt werden. Notwendig ist, die vertraglichen Bedingungen im Hinblick auf die Datenbereitstellung zu bestimmen. Diese

Vertragsbedingungen müssen zwingend den Vorgaben des Data Act (Kapitel III) entsprechen, also insbesondere „fair, angemessen und nichtdiskriminierend" sein. Gewissheit muss auch darüber bestehen, ob und in welcher Höhe eine Gegenleistung für die Datenbereitstellung verlangt werden soll. Dabei muss berücksichtigt werden, dass die Gegenleistung dem Erfordernis der Angemessenheit entspricht. Um die Angemessenheit einer Vergütung prüfen zu können, müssen Hersteller von vernetzten Produkten sich zunächst über den potenziellen Wert der Daten gewahr werden. Dies könnte eine Herausforderung darstellen, da der Wert von Daten je nach Anwendungskontext stark variieren kann und viele Verwertungsszenarien vage oder unvorhersehbar sind. Bei der Datenbereitstellung an Kleinst- oder Kleinunternehmen muss zudem beachtet werden, dass die Gegenleistung nicht höher sein darf als die Kosten, die mit der Bereitstellung der Daten für den Datenempfänger zusammenhängen (Grenzkosten). Bei den Vertragsbedingungen gegenüber Kleinstunternehmen, kleinen oder mittleren Unternehmen, sind zudem die Vorschriften zur Verhinderung von missbräuchlichen Klauseln im Data Act (Kapitel IV) zu beachten.

Durch die Schaffung von Zugangsrechten besteht die Chance, bislang nicht genutzte Datenquellen zu erschließen. Für Forschungsprojekte könnten sich perspektivisch neue Anwendungsfelder bei der Nutzbarmachung von Maschinen- und Produktdaten ergeben. Die Möglichkeit, Daten an Dritte freizugeben, kann zudem die Entwicklung von datenbasierten Geschäftsmodellen begünstigen. Gleichzeitig könnten Unternehmen als Reaktion auf die weitgehenden Verpflichtungen des Data Act auch dazu angehalten sein, ihre Produkte so zu konzipieren, dass überhaupt keine Nutzungsdaten mehr aufgezeichnet werden bzw. dass auf eine Vernetzung der Produkte verzichtet wird. In diesem Falle könnte die Menge an potenziell verfügbaren Daten entgegen der Intention des Verordnungsgebers abnehmen. In Bezug auf die Bereitstellungspflicht von Daten zugunsten der öffentlichen Hand können sich Ansatzpunkte für Forschungsvorhaben ergeben. Zu beachten ist jedoch, dass der Anwendungsbereich der Bereitstellungspflicht sehr eng gefasst ist. Eine Nutzbarmachung der Daten zu Forschungszwecken kommt nur in außergewöhnlichen Notstandslagen in Betracht und auch nur, wenn der Staat die Daten zuvor von den Herstellern angefordert hat. Der tatsächliche Nutzen der Datenbereitstellungspflicht für Forschungsvorhaben lässt sich daher nicht realistisch abschätzen.

3.11 Umsetzungsstand

Nach Vorlage des ersten Kommissionsentwurfs am 22.02.2022 folgte eine Konsultationsphase, in der Unternehmen, Verbraucherorganisationen und Interessensverbände die Möglichkeit hatten, den Rechtsakt zu kommentieren. Es ist sehr wahrscheinlich, dass im anschließenden Trilog-Verfahren Änderungen am Verordnungstext vorgenommen werden. Die Trilog-Verhandlungen werden voraussichtlich frühestens zur Jahreshälfte 2023 abgeschlossen sein. Nach Verabschiedung des Rechtsakts ist eine zwölfmonatige Übergangsfrist vorgesehen.

04

4 DIGITAL SERVICES ACT (DSA)

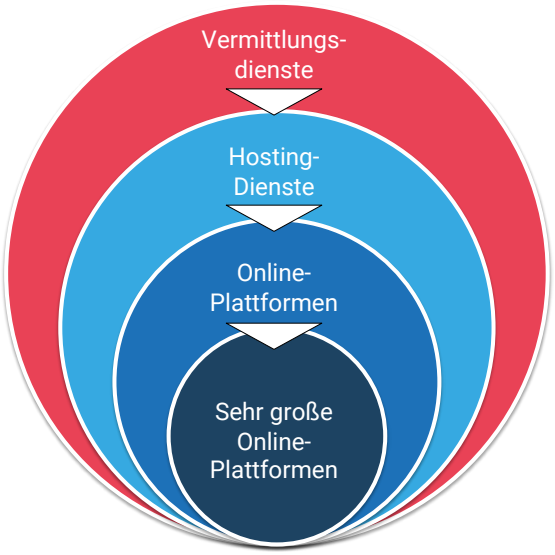
Der Digital Services Act (DSA, Gesetz über digitale Dienste[12]) legt einheitliche Regeln für die Bereitstellung von Vermittlungsdiensten innerhalb der EU fest und löst die seit 20 Jahren bestehende E-Commerce-Richtlinie[13] in Teilen ab. Die Verordnung soll zu einem sicheren, vorhersehbaren und vertrauenswürdigen Online-Umfeld und einem reibungslosen Funktionieren des EU-Binnenmarkts für Vermittlungsdienste beitragen. Hierzu werden

1. Haftungsregeln für Anbieter von Vermittlungsdiensten festgelegt,
2. Sorgfaltspflichten für ein „transparentes und sicheres" Online-Umfeld definiert und
3. Regeln für einen Aufsichts- und Durchsetzungsrahmen bestimmt.

Der DSA wurde gemeinsam mit dem Digital Markets Act konzipiert. Beide Rechtsakte werden die Rolle und die Ausgestaltung von plattformbasierten Diensten in den nächsten Jahren prägen.

4.1 Anwendungsbereich und Adressatenkreis

Der DSA betrifft Anbieter von Vermittlungsdiensten, die ihre Dienste gegenüber Nutzenden innerhalb der EU anbieten. Ob der Anbieter selbst in der EU oder in einem Drittland ansässig ist, spielt dabei keine Rolle. Bei Vermittlungsdiensten wird unterschieden zwischen Anbietern einer „reinen Durchleitung", von „Caching-Leistungen" und von „Hosting-Diensten". Hierdurch wird ein breites Spektrum an Akteuren adressiert. Künftig fallen somit Online-Marktplätze, Hosting-Anbieter, aber auch Anbieter von Cloud- und Messenger-Diensten sowie soziale Netzwerke in den Anwendungsbereich der Verordnung.



Vermittlungsdienste, die über ein Infrastrukturnetz verfügen: Internetanbieter, Domänennamen-Registrierstellen, darunter: …

… Hosting-Dienste wie Cloud- und Webhosting-Dienste, darunter: …

… Online-Plattformen, die Verkäufer und Verbraucher zusammenbringen, wie Online-Marktplätze, App-Stores, Plattformen der kollaborativen Wirtschaft und Social-Media-Plattformen. Darunter: …

… sehr große Online-Plattformen bergen besondere Risiken für die Verbreitung illegaler Inhalte und für Schäden in der Gesellschaft. Für Plattformen, die mehr als zehn Prozent der 450 Millionen Verbraucher Europa erreichen, sind besondere Vorschriften vorgesehen.

Abbildung 9: Unterscheidung von Vermittlungs- und Hosting-Diensten sowie (sehr großen) Online-Plattformen (Quelle: EU-Kommission)

12 https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022R2065&from=en.
13 https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32000L0031&from=DE.

4.2 Haftungsregeln für Anbieter von Vermittlungsdiensten

Zentraler Bestandteil des DSA ist die Festlegung von Haftungsregeln. Konkret werden darin die Bedingungen aufgeführt, unter denen Vermittlungsdienste von der Haftung für Fremdinhalte befreit sind. Voraussetzung für die Inanspruchnahme des Haftungsprivilegs ist es, dass die Vermittlungsdienste neutral bleiben und die ihnen überantworteten Inhalte lediglich technisch verarbeiten, ohne aktiven Einfluss auf diese zu nehmen. Anbieter haben weder eine allgemeine Verpflichtung zur Überwachung der vermittelten Inhalte, noch sind sie verpflichtet, aktiv nach rechtswidrigen Inhalten zu suchen. Eine Haftung ist erst dann vorgesehen, wenn der Anbieter trotz Kenntnis der illegalen Fremdinhalte nicht tätig wird. Im Kern werden damit die in der E-Commerce-Richtlinie vorgesehenen Haftungsprivilegien in den DSA übernommen. Neu hinzugekommen ist die Begünstigung für Fälle, in denen Vermittlungsdienste freiwillig Untersuchungen zur Erkennung und Entfernung von rechtswidrigen Inhalten anstellen (Good-Samaritan-Regelung). Diese Bemühungen werden künftig insofern belohnt, als dass sich auch solche Anbieter auf das Haftungsprivileg berufen können.

4.3 Sorgfaltspflichten

Das dritte Kapitel des DSA enthält ein ausdifferenziertes Regelungswerk hinsichtlich der Sorgfaltspflichten von Vermittlungsdiensten. Eingangs werden allgemein gültige Regeln festgelegt, die für alle Arten von Vermittlungsdiensten gelten. Hierzu gehört etwa die Pflicht zur Einrichtung einer zentralen Kontaktstelle oder die Verpflichtung, in den Geschäftsbedingungen darzulegen, welche Leitlinien, Verfahren, Maßnahmen und Werkzeuge zur Moderation von Inhalten eingesetzt werden. Hinzu kommen Transparenzpflichten wie die Vorgabe, jährliche Transparenzberichte über Lösch- und Sperraktivitäten zu veröffentlichen. Kleinst- oder Kleinunternehmen sind von dieser Verpflichtung ausgenommen. Eine weitere zentrale Verpflichtung betrifft Hosting-Anbieter. Vorgesehen ist insbesondere die Einrichtung eines Melde- und Abhilfeverfahrens, das es Nutzenden ermöglicht, rechtswidrige Inhalte zu melden und entfernen zu lassen.

In Bezug auf Online-Plattformen gelten zusätzliche Bestimmungen. Bei Online-Plattformen handelt es sich um Hostingdienste-Anbieter, die im Auftrag der Nutzenden Informationen speichern und öffentlich verbreiten. Vorgesehen ist etwa die Einrichtung eines internen Beschwerdemanagementsystems für mutmaßlich rechtswidrige Inhalte. Außerdem werden Online-Plattformen verpflichtet, mit zugelassenen außergerichtlichen Streitbeilegungsstellen zusammenzuarbeiten, um Streitigkeiten mit Nutzenden ihrer Dienste beizulegen. Eine weitere Regelung betrifft den Umgang mit sogenannten „Dark Patterns". Dabei handelt es sich um die Gestaltung von Benutzeroberflächen, die den Nutzenden täuschen, manipulieren oder anderweitig maßgeblich in seiner Entscheidungsfindung beeinträchtigen. Genannt werden in diesem Zusammenhang u. a.

- die Hervorhebung von bestimmten Auswahlkriterien, wenn der oder die Nutzende eine Entscheidung treffen muss,
- die wiederholte Aufforderung, eine Auswahl zu treffen, obwohl eine solche Auswahl bereits getroffen wurde, und
- die Gestaltung eines schwierigeren Verfahrens zur Beendigung eines Dienstes als zur Anmeldung.

Daneben gelten für Online-Plattformen weitergehende Pflichten, etwa in Bezug auf die Kennzeichnung von Werbung. Vorgeschrieben ist u. a. die Kennzeichnung, in welchem Namen die Werbung angezeigt wird, wer für die Werbung bezahlt hat und nach welchen Kriterien dem oder der jeweiligen Nutzenden die betreffende Werbung angezeigt wird. Im Hinblick auf den Einsatz von Empfehlungssystemen gelten zudem Transparenzpflichten. Anbieter von Online-Plattformen müssen u. a. erläutern, wie Empfehlungen zustande kommen und wie Nutzende auf die Zusammenstellung von Empfehlungen Einfluss nehmen können.

Angebote von sehr großen Online-Plattformen mit erheblicher Reichweite (mehr als 45 Millionen Nutzende monatlich) sind nach Auffassung des Gesetzgebers mit hohen Risiken verbunden und unterliegen künftig besonders strengen Sorgfaltspflichten. Sehr große Plattformen und Suchmaschinen müssen dabei den Missbrauch ihrer Systeme verhindern, etwa indem sie risikobasierte Maßnahmen ergreifen und ihr Risikomanagementsystem von unabhängiger Seite prüfen lassen.

VERPFLICHTUNGEN	VERMITTLUNGS-DIENSTE	HOSTING-DIENSTE	ONLINE-PLATTFORMEN	SEHR GROSSE PLATTFORMEN
Veröffentlichung eines Transparenzberichtes über Moderation von Inhalten	■	■	■	■
Gestaltung der Nutzungsbedingungen unter Berücksichtigung der Grundrechte der Nutzenden (z. B. Recht auf freie Meinungsäußerung)	■	■	■	■
Zusammenarbeit mit nationalen Behörden (Justiz- oder Verwaltungsbehörden) bei Anordnungen zum Vorgehen gegen rechtswidrige Inhalte	■	■	■	■
Einrichtung einer zentralen Kontaktstelle und Angabe einer gesetzlichen Vertretung bei Anbietern ohne Sitz in der EU	■	■	■	■
Einrichtung eines Melde- und Beseitigungsverfahrens für rechtswidrige Inhalte		■	■	■
Meldepflicht bei Verdacht von Straftaten von Nutzenden der Plattform		■	■	■
Beschwerde- und Rechtsbehelfsmechanismus sowie außergerichtliche Streitbeilegung			■	■
Maßnahmen gegen missbräuchliche Meldungen sowie Möglichkeit zur Gegendarstellung			■	■
Spezielle Pflichten für Marktplätze, z. B. Überprüfung der Berechtigungen von Drittanbietern, Compliance by Design, stichprobenartige Kontrollen, ob Drittanbieter die gesetzlichen Pflichten einhalten			■	■
Verbot von Werbung, die sich gezielt an Kinder richtet oder die besonders sensible Daten (z. B. Gesundheitsdaten) für Profiling oder spezielle personenbezogene Daten nutzt			■	■
Transparenz der Funktionsweise von Empfehlungssystemen			■	■
Transparenz von Online-Werbung gegenüber Nutzenden (z. B. hervorgehobene Kennzeichnung, dass es sich um Werbung handelt)			■	■
Verpflichtung zur Einrichtung eines Risikomanagements und Einrichtung eines Krisenreaktionsmechanismus (Krisenfall kann auf Beschluss der EU-Kommission erlassen werden, etwa bei schwerwiegender Bedrohung der öffentlichen Sicherheit oder der öffentlichen Gesundheit)				■
Externe und unabhängige Prüfung, interne Compliance-Funktion und öffentliche Rechenschaftspflicht				■
Möglichkeit für Nutzende, Empfehlungen anhand von Profiling abzulehnen				■
Einräumung eines Datenzugangs, damit Behörden Einhaltung der Verordnung prüfen können				■
Zusammenarbeit im Krisenfall (z. B. um im Krisenfall die Verbreitung von Falschinformationen zu verhindern)				■
Zusammenarbeit im Krisenfall (z. B. um im Krisenfall die Verbreitung von Falschinformationen zu verhindern)				■

Tabelle 3: Verpflichtungen gestaffelt nach Art des Dienstes bzw. der Plattform (Quelle: EU Kommission)

4.4 Durchsetzung und Sanktionen

Die Durchsetzung der Vorgaben des DSA erfolgt auf zwei Ebenen. Zum einen haben Nutzende ein Recht auf Schadensersatz gegenüber den Anbietern von Vermittlungsdiensten, wenn diese gegen die Verpflichtungen der Verordnung verstoßen. Zum anderen wird die Einhaltung der Verpflichtungen auf nationaler Ebene durch sogenannte „Koordinatoren für digitale Dienste" überwacht. Diese behördlichen Koordinierungsstellen sind befugt, bei Verstößen Sanktionen zu verhängen. Diese Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein. Vorgesehen sind u. a. Geldbußen in Höhe von bis zu sechs Prozent des weltweiten Jahresumsatzes des betreffenden Anbieters im vorangegangenen Geschäftsjahr. Daneben können bei anhaltenden Verstößen Zwangsgelder bis zu einer Höhe von fünf Prozent des durchschnittlichen weltweiten Tagesumsatzes oder der durchschnittlichen weltweiten Tageseinnahmen des betreffenden Anbieters im vorangegangenen Geschäftsjahr festgesetzt werden. Daneben sind für die Durchsetzung der Vorgaben gegenüber großen Online-Plattformen und Suchmaschinen weitere Instrumente vorgesehen, über deren Einsatz vorrangig auf EU-Ebene entschieden wird. Hierfür erhält die EU-Kommission entsprechende Untersuchungs- und Durchsetzungsbefugnisse. Als Sanktionsmechanismen sind auch hier die Verhängung von Buß- und Zwangsgeldern vorgesehen.

4.5 Auswirkungen auf FuE-Projekte

Mit dem DSA wurde ein umfangreiches Gesetzeswerk zur Regulierung von digitalen Vermittlungsdiensten geschaffen. Mit dem Status einer Verordnung hat der DSA auch den Anspruch, die Rahmenbedingungen für die Digitalwirtschaft EU-weit einheitlich zu gestalten und national geprägten Regulierungsansätzen entgegenzuwirken. Die Grundsätze zur Verantwortlichkeit von Vermittlungsdiensten für fremde Inhalte haben sich nur geringfügig geändert. Hier gelten die aus der E-Commerce-Richtlinie bekannten Haftungsprivilegien im Kern weiter. Vermittlungsdienste müssen für Rechtsverletzungen von Dritten grundsätzlich nicht einstehen. Eine Verpflichtung zum Handeln besteht erst nach Kenntniserlangung des jeweiligen Rechtsverstoßes. Das Verfahren zur Meldung und Beseitigung von Rechtsverstößen wird nunmehr verbindlich vorgegeben. Daneben werden zahlreiche Sorgfaltspflichten eingeführt, deren Umfang entsprechend der jeweiligen Betriebsform des Vermittlungsdienstes sowie der Anzahl der Nutzenden des Dienstes proportional zunimmt. Die größten regulatorischen Belastungen entstehen gegenüber großen Online-Diensten und -Suchmaschinen. Daneben sind auch Auswirkungen auf Forschungs- und Entwicklungsprojekte denkbar. Dies hängt davon ab, ob im Rahmen eines Forschungsvorhabens eine Vermittlung oder ein Hosting von Fremdinhalten angedacht ist. In diesem Fall müssen die im DSA vorgesehenen Sorgfaltspflichten umgesetzt werden. Hierfür sollten FuE-Projekte entsprechende Aufwände zur Umsetzung der Vorgaben des DSA in ihrer Arbeitsplanung berücksichtigen. In diesem Zusammenhang ist auch zu prüfen, ob gegebenenfalls Befreiungen von den Sorgfalts- und Transparenzpflichten zugunsten von Klein- und Kleinstunternehmen einschlägig sind.

4.6 Umsetzungsstand

Der DSA wurde am 27.10.2022 im Amtsblatt der Europäischen Union veröffentlicht und gilt ab dem 17.02.2024 unmittelbar in der gesamten EU. Als Verordnung bedarf es keines weiteren nationalen Umsetzungsakts.

05

5 DIGITAL MARKETS ACT (DMA)

Mit dem Gesetz über digitale Märkte (Digital Markets Act, DMA) sollen einheitliche Wettbewerbsbedingungen auf digitalen Märkten geschaffen werden, in denen zentrale, marktmächtige Plattformdienste tätig sind. Daneben soll der Tendenz entgegengewirkt werden, dass die Mitgliedsstaaten der EU nationale Wettbewerbsregeln für Plattformen schaffen, da dies zu einer zusätzlichen Fragmentierung des Binnenmarkts führt.

5.1 Anwendungsbereich und Adressatenkreis

Adressiert werden zentrale Plattformdienste wie Vermittlungsdienste, Suchmaschinen, Betreiber von sozialen Netzwerken, App-Stores, Messenger-Diensten oder Anbieter von Video- oder Cloudplattformen, sofern sie als sogenannte Gatekeeper (Torwächter) benannt wurden. Die Benennung erfolgt durch die EU-Kommission, wenn bestimmte Kriterien erfüllt sind. Berücksichtigt werden dabei u. a. der Einfluss des Unternehmens auf den Binnenmarkt und das Vorliegen einer dauerhaft gefestigten Marktposition. Sind bestimmte quantitative Anforderungen erfüllt, wird die Eigenschaft als Gatekeeper vermutet. Hierzu gehört u. a. der Jahresumsatz (7,5 Milliarden Euro) und die Anzahl der aktiven Nutzenden (45 Millionen). Unternehmen haben die Möglichkeit, gegen die Benennung vorzugehen. Hierzu müssen sie darlegen, dass die Voraussetzungen der Gatekeeper-Eigenschaft trotz Überschreitens der Schwellenwerte nicht gegebenen sind. Bei Erreichen der Schwellenwerte müssen Unternehmen, die zentrale Plattformdienste bereitstellen, dies der EU-Kommission unverzüglich melden.

5.2 Verhaltenspflichten für Gatekeeper

Gatekeeper müssen sich nach Maßgabe des DMA an eine Reihe von Ge- und Verboten halten. Hierzu wird eine Vielzahl von unmittelbar anwendbaren Verpflichtungen statuiert. Verboten sind demnach u. a. die Zusammenführung von personenbezogenen Daten innerhalb von Konzernen. Eine Kombination von Datenbeständen ist nur noch mit der ausdrücklichen Einwilligung der betroffenen Person möglich. Hinzu kommen Ge- und Verbote im Zusammenhang mit Online-Werbung, die für mehr Transparenz und Nachvollziehbarkeit der Dienstleistungs- und Vergütungsstruktur der Gatekeeper im Onlinewerbebereich sorgen sollen. Zusätzlich gibt es eine ganze Reihe von Verbotstatbeständen, die im Kern darauf abzielen, wettbewerbswidrige Vorgehensweisen von großen Plattformen zu unterbinden. Gatekeepern ist es beispielsweise untersagt, eigene Produkte oder Dienste besser zu behandeln als Dienste Dritter, oder Daten gewerblicher Nutzenden, mit denen der Gatekeeper in Wettbewerb steht, für eigene Zwecke zu verwenden.

5.3 Durchsetzung und Sanktionen

Für die Durchsetzung der Vorgaben des DMA ist die EU-Kommission zuständig. Verletzen Gatekeeper eine ihnen obliegende Pflicht, kann die EU-Kommission einen Beschluss wegen Nichteinhaltung erlassen. Im Rahmen des Nichteinhaltungsbeschlusses können Geldbußen bis zu einem Höchstbetrag von zehn Prozent des letzten Jahresumsatzes verhängt werden. Dabei werden die Schwere, die Dauer und eine etwaige Wiederholung der Zuwiderhandlung der Verletzung berücksichtigt. Voraussetzung ist, dass der Gatekeeper die Pflichten vorsätzlich oder fahrlässig verletzt hat. Neben dem behördlichen Sanktionsregime besteht zudem die Möglichkeit, Verstöße privat-

rechtlich zu verfolgen. Das bedeutet, dass auch (gewerbliche und private) Nutzende oder Wettbewerber die Einhaltung der Verordnung klageweise geltend machen können und – sofern hierfür die Voraussetzungen vorliegen – Schadensersatz verlangen können (Podszun et al. 2022, S. 3249).

5.4 Auswirkungen auf FuE-Projekte

Die Auswirkungen des DMA auf Forschungs- und Entwicklungsprojekte ist überschaubar. Der Fokus des Regulierungsvorhabens liegt primär darin, den Aktionsradius von marktmächtigen Plattformkonzernen einzugrenzen und wettbewerbsbeschränkende Geschäftspraktiken zu unterbinden. Hierdurch besteht die Chance, dass die allgemeinen wettbewerblichen Bedingungen, unter denen FuE-Projekte, aber auch kleine und mittlere Unternehmen operieren, verbessert werden. Ob die Verordnung tatsächlich zu offeneren und faireren Märkten führt, lässt sich derzeit noch nicht abschließend bewerten. Maßgeblich wird hierbei sein, inwiefern die im DMA angelegten Kontroll- und Sanktionsmechanismen tatsächlich angewendet werden.

5.5 Umsetzungsstand

Der Digital Markets Act wurde am 12.10.2022 im Amtsblatt der Europäischen Union veröffentlicht und ist am 01.11.2022 in Kraft getreten. Der DMA gilt unmittelbar und ohne weiteren nationalen Umsetzungsakt ab dem 02.05.2023 in der gesamten EU. Ab diesem Datum müssen Unternehmen, die zentrale Plattformdienste anbieten, der EU-Kommission ihren möglichen Status als Gatekeeper mitteilen. Die EU-Kommission wird nach dem anschließenden Prüfverfahren spätestens im August 2023 die ersten Ernennungsbeschlüsse erlassen. Die als Gatekeeper benannten Unternehmen müssen ihren Verpflichtungen dann innerhalb von sechs Monaten nachkommen.

06

6 LITERATURVERZEICHNIS

EU Kommission: Gesetz über digitale Dienste: Mehr Sicherheit und Verantwortung im Online-Umfeld. Online verfügbar unter: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_de, zuletzt geprüft am 09.01.2023.

EU Kommission (2018): Künstliche Intelligenz für Europa. Online verfügbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=COM%3A2018%3A237%3AFIN, zuletzt geprüft am 11.01.2023.

EU Kommission (2020a): Eine europäische Datenstrategie. Online verfügbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52020DC0066&from=DE, zuletzt geprüft am 11.01.2023.

EU Kommission (2020b): Weißbuch zur Künstlichen Intelligenz. Ein europäisches Konzept für Exzellenz und Vertrauen. Online verfügbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52020DC0065&from=DE, zuletzt geprüft am 11.01.2023.

EU Kommission (2021): Digitaler Kompass 2030: Der europäische Weg in die digitale Dekade. Online verfügbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52021DC0118&from=en, zuletzt geprüft am 11.01.2023.

EU Kommission (2022): Künstliche Intelligenz – Exzellenz und Vertrauen. Online verfügbar unter: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/excellence-trust-artificial-intelligence_de, zuletzt aktualisiert am 18.05.2022, zuletzt geprüft am 14.10.2022.

Hennemann, Moritz; Steinrötter, Björn (2022): Data Act – Fundament des neuen EU-Datenwirtschaftsrechts? In: Neue Juristische Wochenschrift 2022 (21), S. 1481–1486.

Hennemann, Moritz; v. Ditfurth, Lukas (2022): Datenintermediäre und Data Governance Act. In: Neue Juristische Wochenschrift 2022 (27), S. 1905–1910.

Klink-Straub, Judith; Straub, Tobias (2022): Data Act als Rahmen für gemeinsame Datennutzung. In: Newsdienst ZD-Aktuell (4), S. 1076.

Podszun, Rupprecht; Bongartz, Philipp; Kirk, Alexander (2022): Digital Markets Act – Neue Regeln für Fairness in der Plattformökonomie. In: Neue Juristische Wochenschrift 2022 (45), S. 3249–3254.

Rat der Europäischen Union (25.11.2022): Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. KI-Verordnung. Online verfügbar unter: https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf, zuletzt geprüft am 09.01.2023.

07

ANHANG

Glossar

BEGRIFF	ERLÄUTERUNG
Artificial Intelligence Act – AI Act	Siehe KI-Verordnung
Data Governance Act (DGA)	Rechtsakt der Europäischen Union, der einen Rahmen schaffen und insbesondere die gemeinsame Nutzung von Daten erleichtern soll. Mit dem Daten-Governance-Rechtsakt hat die Europäische Kommission die Grundlagen für die Schaffung eines europäischen Datenaustauschmodells festgelegt.
Datenempfänger	Juristische oder natürliche Person, die zu Zwecken innerhalb ihrer gewerblichen, geschäftlichen, handwerklichen oder beruflichen Tätigkeit handelt, ohne Nutzer eines Produktes oder verbundenen Dienstes zu sein. Datenempfängern werden vom Dateninhaber Daten bereitgestellt, einschließlich Daten eines Dritten, dem der Dateninhaber auf Verlangen des Nutzers (oder im Einklang mit einer Rechtspflicht aus anderen Rechtsvorschriften der Union oder aus nationalen Rechtsvorschriften zur Umsetzung des Unionsrechts) Daten bereitstellt.
Dateninhaber	Juristische oder natürliche Person, die nach dieser Verordnung, nach anwendbarem Unionsrecht oder nach den anwendbaren nationalen Rechtsvorschriften zur Umsetzung des Unionsrechts berechtigt oder verpflichtet bzw. im Falle nicht personenbezogener Daten und durch die Kontrolle über die technische Konzeption des Produktes und damit verbundener Dienste in der Lage ist, bestimmte Daten bereitzustellen.
Datennutzungsgesetz	Das deutsche Datennutzungsgesetz (DNG) setzt die EU-Vorgaben der Open-Data-Richtlinie um. Daten, die in den Anwendungsbereich des DNG fallen, sollen möglichst „konzeptionell und standardmäßig offen" erstellt und bereitgestellt werden.
Datenvermittlungsdienste	Anbieter, oft auch als Datenintermediär bezeichnet, die (technische, rechtlich o. ä.) Geschäftsbeziehungen zwischen (i. d. R.) Dateninhabern einerseits und Datennutzern andererseits herstellen, um die gemeinsame Datennutzung zu ermöglichen. Dies gilt auch für Zwecke der Ausübung der Rechte betroffener Personen in Bezug auf personenbezogene Daten.
Datenwirtschaft	Begriff zur Beschreibung der ökonomischen Verwertung von Daten. Datenbasierte Geschäftsmodelle stellen Daten als Ressource in den Mittelpunkt der Wertschöpfung.
Durchführungsrechtsakt	Ein Durchführungsrechtsakt ist ein Rechtsakt ohne Gesetzescharakter, in dem detaillierte Vorschriften für die einheitliche Durchführung verbindlicher Rechtsakte der EU festgelegt werden.

BEGRIFF	ERLÄUTERUNG
Europäische Datenstrategie	Mit der Europäischen Datenstrategie hat sich die Europäische Kommission zum Ziel gesetzt, einen europäischen Binnenmarkt für Daten (Daten als Ressource) zu etablieren. Die Datenweitergabe zwischen Unternehmen, Forschenden und öffentlichen Verwaltungen soll so verbessert werden.
FRAND-Bedingung	Als FRAND-Erklärung (FRAND = Fair, Reasonable and Non-Discriminatory terms) bezeichnet man die Erklärung des Patentinhabers gegenüber einer Standardisierungsorganisation, jedem Interessenten zu fairen, angemessenen und nichtdiskriminierenden Bedingungen eine Lizenz zu erteilen.
KI-Strategie (EU)	Strategie der Europäischen Kommission zur europaweiten Förderung exzellenter und vertrauenswürdiger KI-Anwendungen
KI-Verordnung (EU)	Die Verordnung enthält harmonisierte Vorschriften für das Inverkehrbringen, die Inbetriebnahme und die Verwendung von Systemen der Künstlichen Intelligenz in der EU.
Nachnutzung von Daten	Bereits vorliegende Daten – bspw. Daten in einer öffentlichen Verwaltung, erhobene Forschungsdaten etc. – werden erneut in einem anderen Kontext verwendet.
Nutzende eines Dienstes	Natürliche oder juristische Personen, die eine datengetriebene (smarte) Dienstleistung bzw. ein datengetriebenes (smartes) Produkt nutzen. Es entstehen unterschiedliche Daten; durch die Nutzung selbst, als Nebenprodukt der Nutzerinteraktion (z. B. Diagnosedaten) oder durch Aufzeichnung von Umgebungsdaten (bspw. Raumtemperatur).
Verbot von Ausschließlichkeitsvereinbarungen	Verbot der Vergabe von exklusiven (Datennutzungs-)Lizenzen unter Ausschluss weiterer Markteilnehmer.

Kurzübersicht zur aktuellen EU-Gesetzgebung im Bereich Digitalisierung und Datenwirtschaft

AI ACT

WORUM GEHT ES?

Es sollen einheitliche Rahmenbedingungen für die Entwicklung, Vermarktung und Verwendung von KI in der EU geschaffen werden.

Anbieter und Nutzende von KI-Systemen müssen die Vorgaben der KI-Verordnung künftig umsetzen.

Die Verordnung ist anwendbar auf KI-Systeme, also auf Systeme, die Ansätze des maschinellen Lernens sowie logik- und wissensbasierte Ansätze verwenden.

Es sind vier Risikoklassen vorgesehen (unannehmbares, hohes, geringes und minimales Risiko).

KI-Systeme mit einem unannehmbaren Risiko werden verboten, solche mit einem hohen Risiko unterliegen strengen Compliance-Vorgaben.

Systeme mit einem geringen oder minimalen Risiko müssen Transparenzvorgaben erfüllen bzw. unterliegen keinen regulatorischen Vorgaben.

Einhaltung der Verordnung wird behördlich überwacht. Bei Verstößen können Bußgelder verhängt werden.

Unter behördlicher Aufsicht und Leitung können KI-Reallabore eingerichtet werden.

ZENTRALE AUSWIRKUNGEN

Die teils vage Definition von KI-Systemen könnte zu Interpretationsschwierigkeiten bei Anwendern führen.

Produkte und Dienste, die keine Ansätze des maschinellen Lernens sowie logik- und wissensbasierte Ansätze verwenden, werden nicht reguliert.

Für KI-Systeme mit geringem oder minimalem Risiko werden geringe bzw. keine Anforderungen festgelegt.

Anbieter von Hochrisiko-KI-Systemen müssen künftig mit hohem Compliance-Aufwand rechnen.

FuE-Projekte müssen Klarheit darüber schaffen, wer als Anbieter/Nutzer der KI für die Umsetzung der Anforderungen der KI-Verordnung verantwortlich ist.

KI-Reallabore können positive Impulse auf das Innovationsgeschehen haben. Die Rahmenbedingungen sind jedoch sehr restriktiv ausgestaltet und implizieren einen hohen Abstimmungsbedarf mit den Aufsichtsbehörden.

AKTUELLER UMSETZUNGSSTAND

Verabschiedung voraussichtlich im ersten Quartal 2023

Übergangszeit von 36 Monaten

Unmittelbare Geltung voraussichtlich 2026

Gewisser Bestandsschutz für KI-Systeme, die vor 2026 entwickelt und in Betrieb genommen wurden

DATA GOVERNANCE ACT

WORUM GEHT ES?

Die Verfügbarkeit von Daten des öffentlichen Sektors soll verbessert werden, indem Zugangs- und Datenbereitstellungsverfahren vereinheitlicht werden. Betroffen sind öffentliche Stellen wie Behörden, Kommunen, Körperschaften des öffentlichen Rechts.

Schaffung eines Anmelde- und Aufsichtsrahmens für Datenvermittlungsdienste wie Datenmarkplätze, Datentreuhänder oder Ökosystemplattformen

Datenvermittlungsdienste müssen neutral sein und dürfen die vermittelten Daten nicht für eigene Zwecke nutzen oder verwerten.

Datenvermittlungsdienste müssen über eine gesonderte juristische Person bereitgestellt werden. Notwendig sind eine behördliche Anmeldung sowie die Einhaltung von strengen Vorgaben in Bezug auf ihre Tätigkeit.

Die Entstehung von datenaltruistischen Organisationen soll gefördert werden. Vorgesehen ist die Eintragung in ein öffentliches Register. Datenaltruistische Organisationen müssen unabhängig sein und müssen Transparenzvorgaben einhalten.

Verstöße gegen die Verordnung können (z. B. mit Bußgeldern) sanktioniert werden.

ZENTRALE AUSWIRKUNGEN

Die Verfügbarkeit von öffentlich zugänglichen Daten (Open Data) könnte sich perspektivisch verbessern.

Die Regulierung von Datenvermittlungsdiensten hat große Auswirkungen auf die Governance von FuE-Projekten und die darin verfolgten Geschäfts- und Betriebsmodelle.

Datenvermittlungsdienste dürfen Daten nicht monetarisieren. Es muss eine strenge Trennung zwischen Datenmittlung und Datennutzung geben. Der Datenvermittlungsdienst muss über eine gesonderte juristische Person bereitgestellt werden. FuE-Projekte müssen die Bereiche Datenvermittlung/-Angebot datenbasierter Dienste aufteilen. Z. B. ist ein Forschungspartner zuständig für die Datenvermittlungsplattform, der andere für das Angebot von KI-Services. Bei der Geschäftsmodellentwicklung muss berücksichtigt werden, dass das Angebot eines reinen Vermittlungsdienstes möglicherweise finanziell nicht tragfähig ist.

Datenaltruistische Organisationen könnten die Erschließung neuer Datenbestände begünstigen.

AKTUELLER UMSETZUNGSSTAND

Der DGA wurde am 03.06.2022 verabschiedet und ist ab dem 24.09.2023 unmittelbar in der gesamten EU anwendbar.

Für bereits bestehende Datenvermittlungsdienste gilt eine Übergangsfrist bis zum 24.09.2025.

DATA ACT

WORUM GEHT ES?

Der Data Act schafft einen sektorenübergreifenden Governance-Rahmen für die gemeinsame Datennutzung.

Hersteller müssen ihre vernetzten Produkte zugänglich gestalten (Accessibility by Default) und Nutzende über die Datenzugangsmöglichkeiten informieren.

Nutzende haben ein Recht auf Datenzugang zu den von ihnen generierten Daten. Zudem kann auch eine Datenbereitstellung an Dritte verlangt werden.

Die Umstände für die Datenbereitstellung an Dritte ist reguliert, etwa durch Vorgaben hinsichtlich der Vertragsgestaltung.

Der Data Act enthält eine Reihe von Vorschriften, die KMU von dem Anwendungsbereich ausnehmen oder diese vor unfairen Wettbewerbshandlungen schützen sollen.

In Notstandslagen können auch öffentliche Stellen Datenzugang verlangen.

Daneben wird der Wechsel zwischen Cloud-Anbietern erleichtert.

Verstöße können behördlich sanktioniert werden, etwa durch die Verhängung von Bußgeldern.

ZENTRALE AUSWIRKUNGEN

Hersteller müssen ihre Produkte so gestalten, dass die Nutzungsdaten standardmäßig, einfach, sicher und direkt zugänglich sind. Sie müssen auf Verlangen der Nutzenden, diesen und/oder Dritten Daten zugänglich machen (in Notstandslagen auch öffentlichen Stellen). In FuE-Projekten bedarf es einer Abstimmung zwischen den Akteuren, wie die Vorgaben des Data Act umgesetzt werden.

Hersteller müssen die vertraglichen Bedingungen der Datenbereitstellung rechtskonform gestalten. Dies setzt voraus, dass eine mögliche Vergütung festgelegt wird. Das Datenvertragsrecht gewinnt in diesem Zusammenhang erheblich an Bedeutung.

AKTUELLER UMSETZUNGSSTAND

Ein erster Kommissionsentwurf liegt seit dem 22.02.2022 vor.

Die Trilog-Verhandlungen werden voraussichtlich frühestens zur Jahreshälfte 2023 abgeschlossen sein.

Nach Verabschiedung des Rechtsakts ist eine zwölfmonatige Übergangsfrist vorgesehen.

DIGITAL SERVICES ACT

WORUM GEHT ES?

Der Digital Services Act enthält einheitliche Regeln für Anbieter von Vermittlungsdiensten. Es wird unterschieden zwischen Anbietern einer „reinen Durchleitung", von „Caching-Leistungen" und von „Hosting-Diensten.

Es werden Haftungsregeln für Anbieter von Vermittlungsdiensten festgelegt.

Es werden Sorgfaltspflichten für ein „transparentes und sicheres" Online-Umfeld geschaffen.

Es werden Regeln für einen Aufsichts- und Durchsetzungsrahmen bestimmt.

Besonders strenge Anforderungen sind für sehr große Online-Plattformen mit erheblicher Reichweite (mehr als 45 Millionen Nutzende monatlich) vorgesehen.

Die Einhaltung des DSA wird durch behördliche Stellen überwacht. Es besteht die Möglichkeit der Verhängung von Sanktionen in Form von Bußgeldern.

ZENTRALE AUSWIRKUNGEN

Der DSA enthält abhängig von dem angebotenen Dienst eine Vielzahl von Anforderungen, deren Umsetzung mit viel Aufwand verbunden ist.

Betroffen sind jedoch nur Anbieter einer „reinen Durchleitung", von „Caching-Leistungen" und von „Hosting-Diensten". Besonders strenge Vorgaben gelten gegenüber großen Online-Diensten und Suchmaschinen.

Die Haftungsregeln haben sich insgesamt nicht intensiviert. Es gilt nach wie vor der Grundsatz, dass Vermittlungsdienste für rechtswidrige Inhalte ihrer Nutzenden nicht haften.

In Bezug auf die Einhaltung der Sorgfaltspflichten sollten FuE-Projekte entsprechende Aufwände in ihrer Arbeitsplanung berücksichtigen.

AKTUELLER UMSETZUNGSSTAND

Der DSA wurde bereits verabschiedet und findet unmittelbare Anwendung ab dem 17.02.2024.

DIGITAL MARKETS ACT

WORUM GEHT ES?

Mit dem DMA sollen einheitliche Wettbewerbsbedingungen auf digitalen Märkten geschaffen werden, in denen zentrale, marktmächtige Plattformdienste tätig sind.

Adressiert werden zentrale Plattformdienste wie Vermittlungsdienste, Suchmaschinen, Betreiber von sozialen Netzwerken, App-Stores, Messenger-Dienste oder Anbieter von Video- oder Cloudplattformen, sofern sie als sog. Gate-Keeper (Torwächter) benannt wurden.

Die Gate-Keeper-Eigenschaft bemisst sich u.a. nach der Anzahl der aktiven Nutzer (45 Mio.) und dem Jahresumsatz (7,5 Mrd. EUR).

Es werden zahlreiche Ge- und Verbote für Gate-Keeper aufgestellt, etwa im Zusammenhang mit Werbung, Transparenz und in Bezug auf wettbewerbswidrigen Vorgehensweisen.

Für die Durchsetzung der Vorgaben des DMA ist die EU-Kommission zuständig. Die Verhängung von hohen Geldbußen ist als Sanktionsinstrument vorgesehen.

ZENTRALE AUSWIRKUNGEN

Die Auswirkungen auf FuE-Projekte ist überschaubar. Dennoch verbessern sich durch den Rechtsakt die allgemeinen wettbewerblichen Rahmenbedingungen.

AKTUELLER UMSETZUNGSSTAND

Der DMA wurde bereits verabschiedet und gilt unmittelbar ab dem 02.05.2023.