DIE REGULIERUNG VON KÜNSTLICHER INTELLIGENZ UND DATENWIRTSCHAFT

AUSWIRKUNGEN DER AKTUELLEN EU-GESETZGEBUNG AUF 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
01.09.2024

GESTALTUNG
LHLK Agentur für Kommunikation GmbH
Hauptstraße 28
10827 Berlin

BILDER
sdecoret – stock.adobe.com (Titel)

INHALT

EINLEITUNG

Die Europäische Kommission hat am 9. März 2021 ihre Zielvorstellung für die digitale Transformation Europas bis zum Jahr 2030 formuliert. Darin beschreibt sie eine nachhaltige, auf den Menschen ausgerichtete Vision einer digitalen Gesellschaft. Beim Übergang in diese „Digitale Dekade" wird Daten eine Schlüsselrolle zugeschrieben. Die europäische Datenstrategie (EU-Kommission 2020) sieht in diesem Zusammenhang die Schaffung rechtlicher Rahmenbedingungen vor, die den Datenaustausch erleichtern, die Wettbewerbsfähigkeit erhöhen und die digitale Souveränität der EU stärken sollen. Übergeordnetes Ziel ist die Schaffung eines Binnenmarktes für Daten. Bereits zuvor hat die Europäische Kommission mit der Ausarbeitung eines koordinierten Plans für Künstliche Intelligenz (KI) begonnen. Dieser enthält unter anderem Vorschläge zur Schaffung eines EU-weit einheitlichen Rechtsrahmens für KI.

Aufbauend auf diesen konzeptionellen Vorarbeiten wurden in rasantem Tempo Gesetzgebungsvorhaben zur Verwirklichung eines daten- und KI-gestützten Binnenmarktes auf den Weg gebracht, die nach ihrer Verabschiedung ebenso zügig in die Praxis umgesetzt werden müssen. Dies stellt insbesondere Forschungs- und Entwicklungsprojekte (FuE-Projekte), die sich mit der Umsetzung daten- und KI-basierter Technologien befassen, vor große Herausforderungen. Die vorliegende Publikation gibt einen Überblick über fünf zentrale Rechtsakte der Europäischen Union im Bereich KI und Datenwirtschaft:

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

Die Analyse wurde im Rahmen der Begleitforschungsaufträge des Bundesministeriums für Wirtschaft und Klimaschutz (BMWK) zu den Technologieprogrammen „KI-Innovationswettbewerb" und „Smarte Datenwirtschaft" durchgeführt. Die Darstellung der Rechtsakte konzentriert sich daher jeweils auf die folgenden Fragen zu den in den Programmen geförderten FuE-Projekten:

- Worum geht es? (Anwendungsbereich)
- Wen betrifft die Regelung? (Adressatenkreis)
- Wie wird die Einhaltung kontrolliert? (Durchsetzung und Sanktionen)
- Welche Auswirkungen haben die Regelungen auf FuE-Projekte?

Im Anhang finden sich ein Glossar der zentralen Begriffe sowie eine Kurzübersicht über Inhalte und Auswirkungen der betrachteten Rechtsakte auf FuE-Projekte.

Die Darstellungen basieren auf dem aktuellen Stand der jeweiligen Gesetzgebungsverfahren (Stand: Juli 2024).

Die vorliegende zweite Auflage ersetzt die bisherige erste Auflage vom Februar 2023. Der Anlass für die Neuauflage ist in den zum Teil erheblichen Änderungen der hier behandelten Rechtsakte im Laufe des Gesetzgebungsverfahrens zu verorten, insbesondere beim AI Act und Data Act. Des Weiteren hat der deutsche Gesetzgeber mit der Umsetzung der einzelnen Rechtsakte begonnen, was bedeutet, dass derzeit entsprechende nationale Gesetze geschaffen werden bzw. bereits verabschiedet wurden, die insbesondere Fragen der Marktüberwachung und Durchsetzung der EU-Vorgaben betreffen.

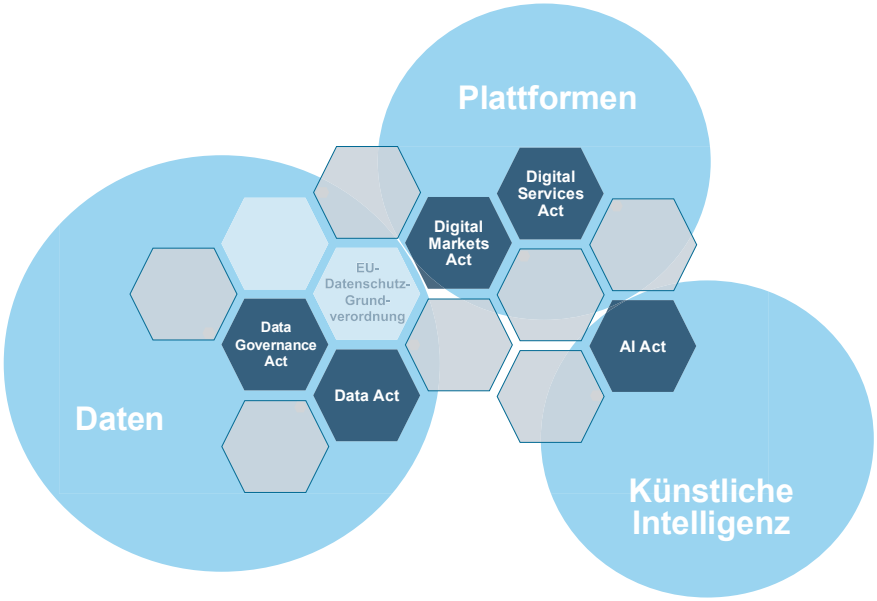


Abbildung 1: Die aktuelle EU-Gesetzgebung im Bereich Künstliche Intelligenz, Datenwirtschaft und Plattformregulierung

01

1 ARTIFICIAL INTELLIGENCE ACT (AI ACT)

Mit der KI-Verordnung[1] (Artificial Intelligence Act oder AI Act) wird ein EU-weit einheitlicher Rechtsrahmen für die Entwicklung, Vermarktung und Nutzung von Künstlicher Intelligenz geschaffen. Die Initiative für den Legislativvorschlag geht auf die 2018 veröffentlichte Europäische KI-Strategie zurück. Die Vorarbeiten für die Verordnung basieren auf den Erkenntnissen des Weißbuchs zur Künstlichen Intelligenz (EU Kommission 2020). Darin wurden unter anderem 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 finden sich im Verordnungsentwurf wieder (siehe Abschnitt 1.3).

1.1 Anwendungsbereich

Die KI-Verordnung legt allgemeine Regeln für das Inverkehrbringen, die Inbetriebnahme und die Verwendung von Systemen Künstlicher Intelligenz (KI-Systeme) fest. Zentraler Anknüpfungspunkt für die Anwendbarkeit der KI-Verordnung ist daher das Vorliegen eines KI-Systems. Wie dieser Schlüsselbegriff zu definieren ist, wurde bis zuletzt intensiv diskutiert. Die Herausforderung bestand darin, eine klare, rechtssichere und zugleich technologieoffene Formulierung zu finden. Im Ergebnis einigte man sich auf bestimmte Schlüsselmerkmale von KI-Systemen, die sie von herkömmlicher Software und einfacheren Programmieransätzen unterscheiden. Dazu gehört zunächst die Fähigkeit von KI-Systemen, mit unterschiedlichen Autonomiegraden zu arbeiten. Das bedeutet, dass KI-Systeme bis zu einem gewissen Grad unabhängig von menschlichen Eingriffen sind und auch ohne menschliches Zutun funktionieren können. Darüber hinaus sind KI-Systeme adaptiv, d. h., sie sind in der Lage, sich an neue Situationen und Anforderungen während der Nutzung anzupassen; sie sind also lernfähig. Ein weiteres zentrales Merkmal von KI-Systemen ist die Modellinferenz, d. h. die Fähigkeit, aus Daten Schlussfolgerungen oder Erkenntnisse zu ziehen. Diese Fähigkeit – auch als Inferenzfähigkeit bezeichnet – bezieht sich auf den Prozess der Ergebnisgewinnung: KI-Systeme sind demnach in der Lage, aus Eingaben oder basierend auf Daten Vorhersagen, Empfehlungen oder Entscheidungen abzuleiten.

Ein KI-System

- ist ein maschinenbasiertes System,
- arbeitet mit unterschiedlichen Autonomiegraden,
- ist anpassungsfähig,
- kann aus Eingaben Schlussfolgerungen ziehen und
- erzeugt daraus Output wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen.
- Der Output beeinflusst die physische oder virtuelle Umgebung.

Ein wesentliches Anliegen des Verordnungsgebers bei der Festlegung der Definition war die internationale Anschlussfähigkeit. Aus diesem Grund orientiert sich die Definition weitgehend an den

1 Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz), https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401689

Vorgaben der OECD. Darüber hinaus sollen mögliche Rechtsunsicherheiten bei der praktischen Anwendung der Definition vermieden werden. In diesem Zusammenhang wird die Europäische Kommission Leitlinien für die praktische Umsetzung der KI-Verordnung entwickeln. Diese werden auch die Anwendung der Definition von KI-Systemen umfassen. Besonderes Augenmerk soll dabei auf die Bedürfnisse von KMU, Start-ups, Behörden und stark betroffenen Sektoren gelegt werden.

Ausnahme für KI-Systeme unter freier oder offener Lizenz
KI-Systeme, die unter einer freien oder offenen Lizenz veröffentlicht werden, sollen vom Anwendungsbereich der KI-Verordnung ausgenommen werden. Solchen KI-Systemen wird eine hohe Bedeutung für Forschung und Innovation beigemessen. Zu beachten ist jedoch, dass die Ausnahme nur für KI-Systeme gilt, die nicht verboten oder hochriskant sind (siehe Risikoklassen 1.3).

Ausnahmeregelungen für Forschung und Entwicklung
KI-Systeme sind vom Anwendungsbereich der Verordnung ausgenommen, wenn sie ausschließlich für Zwecke der wissenschaftlichen Forschung und Entwicklung geschaffen und in Betrieb genommen werden. Die Ausnahmeregelung in Art. 2 Abs. 6 KI-VO soll sicherstellen, dass Innovationen nicht durch übermäßige regulatorische Hürden behindert werden. Unternehmen und Forschungsprojekte können die Ausnahmeregelung in Anspruch nehmen, wenn sichergestellt ist, dass das KI-System alleinig Forschungs- und Entwicklungszwecken dient. Jede Abweichung von dieser Zweckbestimmung, z. B. durch die Verfolgung (auch nur teilweise) kommerzieller Ziele, führt zum Ausschluss des Forschungs- und Entwicklungsprivilegs. Eine zentrale Herausforderung besteht somit darin, den Zweck der Forschungs- und Entwicklungstätigkeit klar zu definieren und von einer möglichen kommerziellen Verwertung abzugrenzen. Dies wird nicht immer trennscharf möglich sein, da Forschungs- und Entwicklungsaktivitäten häufig in eine kommerzielle Nutzung münden. Um den Anschein einer missbräuchlichen Umgehung der KI-Verordnung zu vermeiden, sollte der Forschungs- und Entwicklungscharakter des jeweiligen Vorhabens herausgestellt und entsprechend dokumentiert werden.

Die KI-Verordnung nimmt darüber hinaus Forschungs-, Erprobungs- oder Entwicklungstätigkeiten von ihrem Anwendungsbereich aus. Im Gegensatz zur oben genannten FuE-Ausnahme, die nur für KI-Systeme gilt, die ausschließlich für Forschungs- und Entwicklungszwecke entwickelt und eingesetzt werden, bezieht sich die zweite Ausnahme nach Art. 2 Abs. 8 KI-VO auf alle Forschungs-, Test- oder Entwicklungstätigkeiten im Zusammenhang mit KI-Systemen oder KI-Modellen, bevor diese auf den Markt gebracht oder in Betrieb genommen werden. Dies umfasst auch kommerzielle Forschungs- und Entwicklungstätigkeiten. Die Befreiung ist zeitlich befristet. Spätestens mit dem Inverkehrbringen oder der Inbetriebnahme des KI-Systems müssen alle Anforderungen der KI-Verordnung vollständig erfüllt sein. Darüber hinaus gilt die Ausnahme nur für den Anwendungsbereich der KI-Verordnung selbst; eine Freistellung von anderen regulatorischen Anforderungen erfolgt nicht. Alle Aktivitäten müssen daher im Einklang mit dem sonstigen anwendbaren Unionsrecht durchgeführt werden. Eine wichtige Einschränkung betrifft die Erprobung von KI-Systemen unter Realbedingungen. Da sich die Risiken von KI bereits in der Phase vor der Markteinführung materialisieren können, wird die Erprobung unter realen Einsatzbedingungen explizit ausgeschlossen. Damit soll sichergestellt werden, dass mögliche Risiken und Gefahren, die durch unzureichend erprobte KI-Systeme in realen Umgebungen entstehen können, rechtzeitig erkannt und vermieden werden können. Konkret bedeutet dies, dass KI-Systeme vor ihrem Einsatz in realen Einsatzszenarien alle regulatorischen Anforderungen erfüllen müssen, um die Sicherheit und Zuverlässigkeit im praktischen Einsatz zu gewährleisten.

1.2 Adressatenkreis

Die Verordnung nimmt in erster Linie die Anbieter von KI-Systemen in die Pflicht. Anbieter sind natürliche oder juristische Personen, aber auch Behörden, Einrichtungen oder andere Stellen, die ein KI-System entwickeln und unter ihrem eigenen Namen oder ihrer eigenen Marke in Verkehr bringen oder in Betrieb nehmen. Anbieter können auch solche Akteure sein, die die Entwicklung eines KI-Systems in Auftrag geben. Anbieter unterliegen den Regelungen der KI-Verordnung auch dann, wenn sie KI-Systeme kostenlos zur Verfügung stellen. Auf die Entgeltlichkeit der Bereitstellung kommt es also nicht an. Darüber hinaus gilt die KI-Verordnung auch für Betreiber von KI-Systemen, also für diejenigen Akteure, die ein KI-System in eigener Verantwortung einsetzen. Neben Anbietern und Betreibern werden weitere andere Akteure entlang der KI-Wertschöpfungskette adressiert. In diesem Zusammenhang sind beispielsweise Pflichten für Akteure vorgesehen, die mit KI-Systemen von Unternehmen außerhalb der EU handeln oder diese in die EU einführen. Damit soll eine durchgängige Verantwortlichkeit für die Einhaltung der Anforderungen der KI-Verordnung sichergestellt werden. Dabei unterscheiden sich die Pflichten der jeweiligen Akteure auch nach ihrem Einflussbereich und ihrer Möglichkeit, Risiken zu beeinflussen. Der in der KI-Verordnung verankerte risikobasierte Ansatz stellt dabei auf das von KI-Systemen ausgehende Risiko ab.

1.3 Risikoklassen

Die KI-Verordnung sieht insgesamt vier Risikoklassen vor (unannehmbares, hohes, geringes und minimales Risiko). KI-Systeme mit unannehmbarem Risiko sind verboten. KI-Systeme mit hohem Risiko müssen zahlreiche Mindestanforderungen erfüllen, bevor sie in Verkehr gebracht oder in Betrieb genommen werden dürfen. KI-Systeme mit begrenztem oder minimalem Risiko müssen hingegen lediglich Transparenzanforderungen erfüllen bzw. unterliegen keinen regulatorischen Anforderungen.

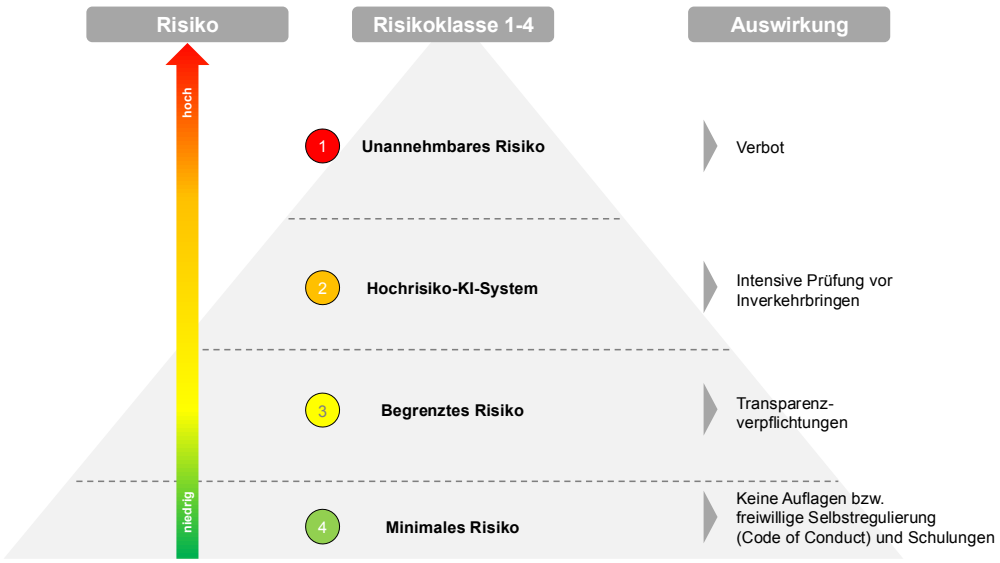


Abbildung 2: Übersicht zu den Risikoklassen der KI-Verordnung

1.3.1 RISIKOKLASSE 1: UNANNEHMBARES RISIKO

Bestimmte KI-Praktiken sind mit unannehmbaren Risiken verbunden und unterliegen einem Verbot. Dazu gehören Techniken, die darauf abzielen, Menschen zu manipulieren oder die Schwäche oder Schutzbedürftigkeit bestimmter (vulnerabler) Personengruppen auszunutzen. Dabei muss das KI-System das Verhalten dieser Personen oder Personengruppen so beeinflussen, dass Schäden (physischer oder psychischer Art) verursacht werden. Verboten sind auch 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 Mittelpunkt der Verordnung steht die Regulierung sogenannter Hochrisiko-KI-Systeme. Dabei handelt es sich um KI-Systeme, deren Ausfall oder Fehlfunktion besonders schwerwiegende Folgen für die Sicherheit, die Gesundheit und die Grundrechte natürlicher Personen hätte. Solche Hochrisiko-KI-Systeme sollen nur dann in Verkehr gebracht oder in Betrieb genommen werden dürfen, wenn sie bestimmte, nachprüfbare Anforderungen erfüllen. Die Einstufung als KI-System mit hohem Risiko betrifft drei Fälle:

Fall 1: „KI ist ein Produkt oder eine Sicherheitskomponente eines Produkts und unterliegt einer EU-Sicherheitsregulierung."

Anhang I Abschnitt A der KI-Verordnung enthält einen Katalog einschlägiger EU-Rechtsakte. Diese umfassen vorrangig Richtlinien und Verordnungen, die das Inverkehrbringen oder die Inbetriebnahme besonders sicherheitsrelevanter Produkte regeln, wie Maschinen, Spielzeug oder Medizinprodukte. KI-Systeme, die als Produkt oder Produktbestandteil aufgrund eines dieser Rechtsakte einer Konformitätsbewertung durch Dritte unterliegen, gelten automatisch als Hochrisiko-KI-Systeme.

Fall 2: „KI ist ein Produkt oder eine Sicherheitskomponente eines Produkts – in Bereichen mit bereits bestehenden Prüf- und Zulassungsverfahren."

Anhang I enthält in Abschnitt B eine Liste von EU-Richtlinien und Verordnungen zur Produktsicherheit. Fällt das KI-System in den Regelungsbereich eines dort aufgeführten Rechtsaktes, ist die KI-Verordnung weitestgehend nicht direkt anwendbar. Grund hierfür ist, dass in den adressierten Bereichen (z. B. Typgenehmigung von Kraftfahrzeugen oder Sicherheit in der Zivilluftfahrt) bereits bestehende Prüf- und Zulassungsverfahren existieren. Der Verordnungsgeber will daher nicht unnötig in bereits etablierte und ausdifferenzierte Regelungssysteme eingreifen. Auch wenn KI-Systeme, die unter Anhang I Abschnitt B fallen, weitestgehend vom Anwendungsbereich ausgenommen sind, sollten Hersteller in den betroffenen Bereichen zukünftig dennoch die Vorgaben der KI-Verordnung berücksichtigen. Denn die sektorspezifischen Sicherheitsvorschriften werden so angepasst, dass die Anforderungen der KI-Verordnung für Hochrisiko-KI-Systeme bei der Fortschreibung dieser Rechtsakte zu berücksichtigen sind. Daraus ergeben sich zumindest mittelfristig Auswirkungen auf die Ausgestaltung dieser Produkte bzw. Produktkomponenten.

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

KI-Systeme gelten als hochriskant, wenn sie in einem der in **Anhang III** aufgeführten Bereiche eingesetzt werden, wie z. B. in kritischen Infrastrukturen, Bildung, Beschäftigung, Strafverfolgung, Migration oder Rechtspflege. Nicht jeder Einsatz von KI in diesen Bereichen führt jedoch automatisch zur Einstufung als Hochrisiko-KI-System. Entscheidend ist, ob die beabsichtigte Verwendung tatsächlich einem der im Anhang III genannten Anwendungsfälle entspricht.

Selbst wenn die beabsichtigte Verwendung einem dieser Anwendungsfälle entspricht, kann die Einstufung als Hochrisiko-KI-System vermieden werden, wenn keine erhebliche Gefahr für die Gesundheit, Sicherheit oder Grundrechte von Personen besteht, insbesondere, wenn der KI-Einsatz den Ausgang von Entscheidungsprozessen nicht wesentlich beeinflusst. Hierzu hat der Verordnungsgeber eine Ausnahmeregelung geschaffen, wonach Anhang-III-Systeme nicht als hochriskant angesehen werden, wenn eine der folgenden Bedingungen erfüllt ist:

a) **Spezialisierte Aufgaben:** Das KI-System führt spezifische und eng definierte Aufgaben aus.
b) **Verbesserung von Ergebnissen:** Das KI-System wird eingesetzt, um das Ergebnis einer bereits abgeschlossenen menschlichen Tätigkeit zu verbessern.
c) **Erkennung von Entscheidungsmustern:** Das KI-System analysiert, wie Entscheidungen getroffen wurden, um Unregelmäßigkeiten oder Veränderungen zu erkennen, ersetzt aber nicht die menschliche Entscheidung und wird immer von Menschen überprüft.
d) **Vorbereitende Aufgaben:** Das KI-System übernimmt vorbereitende Schritte für eine Bewertung oder Entscheidung, führt aber keine tiefer gehende Analyse oder Bewertung von Personen durch.

Die Ausnahmeregelung gewährleistet, dass nicht jedes Anwendungsszenario nach Anhang III zwangsläufig dazu führt, dass ein KI-System als hochriskant eingestuft wird. Anbietern von Anhang-III-Systemen wird damit die Möglichkeit eröffnet, durch eine entsprechende Ausgestaltung eine Klassifikation ihrer Anwendung als Hochrisiko-KI-System zu vermeiden.

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 Algorithmen-gestützte Kategorisierung von Personen, beispielsweise im Rahmen der Strafverfolgung oder Grenzkontrolle, Migration, Asylverfahren Straffälligkeitsüberprüfung/Überprüfung von Bewährungsauflagen
- Rechtspflege (z. B. bei der Auslegung von Sachverhalten und Gesetzen)

Hinweis zur praktischen Umsetzung

Zur Unterstützung von KI-Anbietern wird die Europäische Kommission nach Inkrafttreten der KI-Verordnung Leitlinien für die praktische Umsetzung der Risikoklassifizierung entwickeln. Dazu gehört auch eine umfangreiche Liste von Praxisbeispielen. Unternehmen und Forschungsprojekte sollten die Aktivitäten der EU-Kommission bei der Erstellung der Leitlinien verfolgen und sich ggf. an den dort getroffenen Vorgaben orientieren.

Eine zentrale Aufgabe für Unternehmen und Forschungsprojekte ist die Risikoklassifizierung ihrer KI-Systeme. Die Einstufung als Hochrisiko-KI-System kann im Einzelfall durch eine entsprechende Gestaltung des KI-Systems abgewendet werden. Wichtig ist jedoch, dass diejenigen, die sich auf die Ausnahmeregelung berufen, nach der Anhang-III-Systeme doch nicht als hochriskant eingestuft zu werden, verpflichtet sind, die Gründe dafür zu dokumentieren, bevor das KI-System in Verkehr gebracht wird. Darüber hinaus besteht die Pflicht, diese KI-Systeme in einer zentralen EU-Datenbank zu registrieren. Auf Anfrage der Aufsichtsbehörden muss der Anbieter des KI-Systems nachweisen können, warum die Voraussetzungen des Ausnahmetatbestandes erfüllt sind. Die Ausnahmeregelung entlastet den Anbieter also insofern, als dass die Anforderungen an Hochrisiko-KI-Systeme nicht umgesetzt werden müssen. Gleichzeitig muss jedoch sichergestellt werden, dass der Anbieter das Vorliegen von Voraussetzungen für die Ausnahmeregelung gut begründen kann.

1.3.2.1 Mindestanforderungen an Hochrisiko-KI-Systeme

KI-Systeme mit hohem Risiko müssen gemäß Kapitel III Abschnitt 2 der KI-Verordnung Sicherheits- und Transparenzanforderungen erfüllen. Durch die Festlegung von Mindestanforderungen sollen die Risiken für Gesundheit, Sicherheit und Grundrechte, die sich aus dem Einsatz des KI-Systems ergeben, verringert werden. Bei der Erfüllung der Mindestanforderungen soll der Verwendungszweck des Hochrisiko-KI-Systems berücksichtigt werden. Je nach Verwendungszweck und den individuellen Risiken des KI-Systems können sich daher unterschiedliche Schwerpunkte bei der Umsetzung der Mindestanforderungen ergeben.

Mindestanforderungen für Hochrisiko-KI-Systeme

Die Mindestanforderungen sind:

- Einrichtung eines Risikomanagementsystems, das eine Risikobewertung und Maßnahmen zur Risikominderung oder -beseitigung umfasst,
- Sicherstellung der Datenqualität, insbesondere durch Qualitätsanforderungen für Trainings-, Validierungs- und Testdatensätze,
- technische Dokumentation zum Nachweis der Erfüllung der Mindestanforderungen,
- automatische Protokollierung von Vorgängen und Ereignissen während des Betriebs,
- Einhaltung von Transparenzpflichten, um die Ergebnisse des KI-Systems interpretieren und nutzen zu können,
- Bereitstellung einer für den Betreiber verständlichen Gebrauchsanweisung,
- Verpflichtung, das Hochrisiko-KI-System so zu entwickeln und zu gestalten, dass eine menschliche Überwachung während der gesamten Nutzungsdauer gewährleistet ist,
- Gewährleistung der Robustheit, Sicherheit und Genauigkeit des KI-Systems.

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

Anbieter von Hochrisiko-KI-Systemen müssen zunächst die Einhaltung der Mindestanforderungen an Hochrisiko-KI-Systeme (siehe oben) sicherstellen. Eine zentrale Pflicht ist dabei die Einrichtung eines Qualitätsmanagementsystems, das durch konkret zu benennende Verfahren und Anweisungen die Einhaltung der Vorgaben der Verordnung sicherstellt. Dies umfasst Aspekte wie die Darstellung von Prüf-, Test- und Validierungsverfahren oder Ausführungen zum Datenmanagement. Darüber hinaus sind Verfahren zur Überwachung des KI-Systems nach dem Inverkehrbringen sowie Verfahren zur Meldung schwerwiegender Vorkommnisse und Störungen festzulegen. Die Anforderungen an das Qualitätsmanagementsystem sind an die Größe der Organisation des Anbieters anzupassen. Dies bedeutet, dass z. B. kleinere Anbieter nicht den gleichen Umfang an Qualitätsmanagementprozessen nachweisen müssen wie etwa große Unternehmen. Damit soll eine flexible Umsetzung der Anforderungen unter Berücksichtigung der individuellen Leistungsfähigkeit des jeweiligen Anbieters gewährleistet werden.

Darüber hinaus besteht die Pflicht zur Durchführung eines Konformitätsbewertungsverfahrens. Für KI-Systeme nach Anhang III ist ein internes Konformitätsbewertungsverfahren ausreichend (mit Ausnahme biometrischer Fernidentifizierungssysteme). Bei Anhang-I-KI-Systemen (Abschnitt A) befolgt der Anbieter die einschlägigen Konformitätsbewertungsverfahren, die nach den dort genannten Rechtsakten erforderlich sind. Nach erfolgreicher Konformitätsbewertung erstellt der Anbieter eine EU-Konformitätserklärung und bringt die CE-Kennzeichnung an. Darüber hinaus besteht die Verpflichtung, das Hochrisiko-KI-System in einer öffentlich zugänglichen EU-Datenbank zu registrieren. Diese Datenbank wird von der EU-Kommission eingerichtet und gepflegt. Es ist zu beachten, dass bei wesentlichen Änderungen des KI-Systems eine erneute Konformitätsbewertung erforderlich ist.

Abbildung 3: Ablauf des Konformitätsbewertungsverfahrens

1.3.3 RISIKOKLASSE 3: BEGRENZTES RISIKO

Bei KI-Systemen mit spezifischen Manipulationsrisiken sind – unabhängig von der Einstufung als Hochrisiko-KI-System – Transparenzpflichten zu beachten. Beispielsweise müssen Personen informiert werden, wenn sie mit einem KI-System interagieren, etwa im Rahmen der Bearbeitung von Kundenanfragen (z. B. Chatbots). Davon 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. Darüber hinaus sind KI-Systeme zu kennzeichnen, die Bild-, Ton- oder Videoinhalte von Personen, Gegenständen, Orten oder Ereignissen erzeugen oder manipulieren. Damit hat der Verordnungsgeber vor allem sogenannte Deepfakes im Blick. Solche KI-Systeme 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 besonderen Anforderungen. Die Anbieter solcher Systeme können sich jedoch freiwillig Verhaltenskodizes unterwerfen. Darüber hinaus wird sowohl von den Anbietern als auch von den Betreibern verlangt, dass ihr Personal über ausreichende Kenntnisse im Umgang mit KI-Systemen verfügt, wobei technische Kenntnisse, die Erfahrung, die Ausbildung und der Nutzungskontext zu berücksichtigen sind.

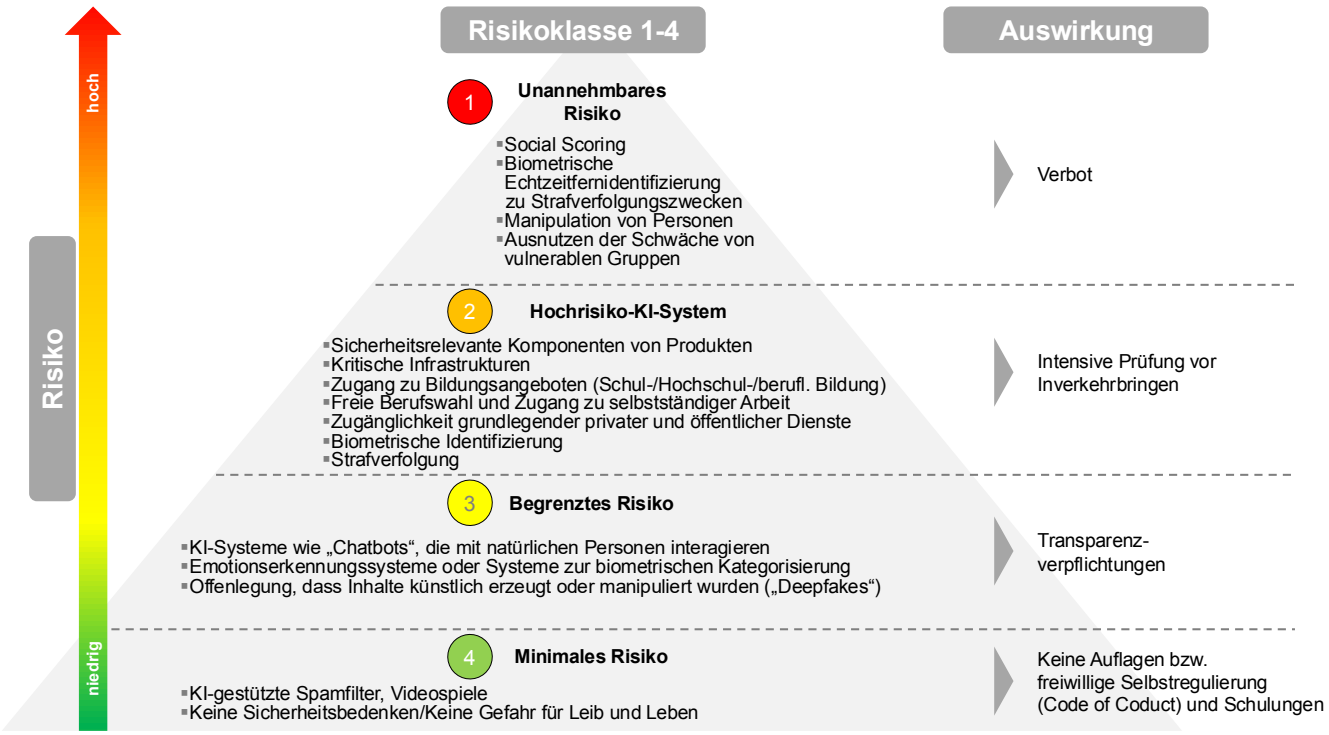


Abbildung 4: Die Risikoklassen 1 bis 4 der KI-Verordnung mit Beispielen und Auswirkungen

1.4 Sonderfall: General Purpose AI Models

Die sprunghafte Entwicklung von generativen KI-Systemen wie ChatGPT oder Midjourney sowie deren kurzfristige Markteinführung stellten den Verordnungsgeber im Laufe des Legislativprozesses vor erhebliche Herausforderungen. Zum Zeitpunkt des ersten Entwurfs der KI-Verordnung war das Ausmaß der technologischen Entwicklungen im Bereich der Text-zu-Text- und Text-zu-Bild-Generatoren noch nicht absehbar. Dementsprechend gab es auch keine technologiespezifischen Regelungen für diese Systeme. Die Zweckoffenheit von generativen KI-Systemen und den zugrundeliegenden Basismodellen erwies sich als zusätzliche Herausforderung und erschwerte die Integration in die Risikometrik des ursprünglichen Verordnungsentwurfs. Je nach Anwendungskontext können generative KI-Systeme prinzipiell alle Risikoklassen abdecken. Vor diesem Hintergrund gestalteten sich die Verhandlungen zwischen der Europäischen Kommission, dem Europäischen Rat und dem Europäischen Parlament schwierig. In der finalen Fassung der KI-Verordnung einigte man sich darauf, bereichsspezifische Regelungen für sogenannte General Purpose AI Models (GPAI) zu schaffen. Diese auf große Datenmengen trainierte KI-Modelle zeichnen sich durch ihre Vielseitigkeit aus und lassen sich leicht in andere Systeme oder Anwendungen integrieren. Die KI-Verordnung sieht unter anderem vor, dass Anbieter von GPAI technische Dokumentationen erstellen und aktualisieren, anderen Anbietern Informationen über die Funktionsweise des KI-Models zur Verfügung stellen und urheberrechtliche Bestimmungen beachten müssen. Für GPAI mit systemischen Risiken gelten weitergehende Anforderungen wie die Durchführung einer Modell- und Risikobewertung, die Gewährleistung der Cybersicherheit und die Meldepflicht für schwerwiegende Vorfälle. Für die Einstufung wird unter anderem die für das Training des KI-Modells eingesetzte Rechenleistung (mehr als 10^25 FLOPs) berücksichtigt. Aus Sicht von Unternehmen und Forschungsprojekten besteht insbesondere dann Handlungsbedarf, wenn ein GPAI in ein als hochriskant einzustufendes KI-System integriert werden soll. In diesem Fall wechselt der Betreiber des KI-Systems in die Rolle des Anbieters und unterliegt damit in vollem Umfang den Mindestanforderungen des Kapitels III der KI-Verordnung. Die Umsetzung der Anbieterpflichten kann insofern eine Herausforderung darstellen, als dass der GPAI nutzende Anbieter nicht über alle Informationen verfügt, die für eine adäquate Risikoeinschätzung erforderlich sind. Diesem Umstand versucht der Verordnungsgeber dadurch zu begegnen, dass der Anbieter des GPAI die zur Erfüllung der in der KI-Verordnung festgelegten Pflichten erforderlichen Informationen zur Verfügung stellt. Dadurch soll sichergestellt werden, dass der neue Anbieter des KI-Systems über alle notwendigen Informationen verfügt, um die gesetzlichen Anforderungen zu erfüllen und eine umfassende Risikoeinschätzung durchführen zu können.

1.5 KI-Reallabore und Testen unter Realbedingungen

Als zentrales Element der Innovationsförderung sieht die KI-Verordnung die Einrichtung von Reallaboren („AI regulatory sandboxes“) vor. Im Rahmen dieser Experimentierräume soll die Entwicklung, Erprobung und Validierung innovativer KI-Systeme vorangetrieben werden. Die Mitgliedstaaten sind aufgefordert, 24 Monate nach Verabschiedung der KI-Verordnung ein oder mehrere solcher KI-Reallabore einzurichten. Die Durchführung und Überwachung erfolgt unter Aufsicht und Anleitung der zuständigen Behörden. Zu beachten ist, dass die Regelungen zu und die Durchführung von Reallaboren keine Befreiung von der KI-Verordnung bedeuten. Potenzielle Anbieter von KI-Systemen bleiben in vollem Umfang für die Einhaltung der rechtlichen Anforderungen verantwortlich. Die neuen KI-Reallabore zielen vielmehr darauf ab, eine kontrollierte Experi-

mentier- und Testumgebung in der Entwicklungs- und Vorvermarktungsphase zu schaffen und damit die Rechtssicherheit zu erhöhen. Hierzu ist vorgesehen, dass die Anbieter zwar für etwaige Schäden Dritter haften, jedoch von der Verhängung behördlicher Bußgelder abgesehen wird, wenn der Plan und die Bedingungen für die Teilnahme am KI-Reallabor eingehalten und die Hinweise der Behörde befolgt werden. Darüber hinaus ergeben sich im Rahmen von KI-Reallaboren neue Spielräume bei der Verarbeitung personenbezogener Daten. Bisher durften bereits erhobene personenbezogene Daten nur in engen Grenzen weiterverwendet werden. Unter anderem musste sichergestellt werden, dass der Zweck der Weiterverwendung in engem Zusammenhang mit dem ursprünglichen Erhebungszweck steht. Dies führte häufig dazu, dass eine sekundäre Nutzung personenbezogener Daten, etwa zum Training von KI-Modellen, ausgeschlossen war. Art. 59 der KI-Verordnung erlaubt nun die Weiterverarbeitung rechtmäßig erhobener personenbezogener Daten, sofern die Entwicklung in bestimmten, vom Verordnungsgeber festgelegten Bereichen erfolgt. Zu den privilegierten Anwendungsbereichen zählen unter anderem die öffentliche Sicherheit und Gesundheit, der Umweltschutz, die Energie- und Infrastruktursicherheit oder die öffentliche Verwaltung. Dies ist jedoch nur zulässig, wenn die Verarbeitung auch erforderlich ist, d. h., die Entwicklung nicht mit anonymisierten, synthetischen oder anderen nicht personenbezogenen Daten möglich ist. Zum Schutz personenbezogener Daten in KI-Reallaboren sind die Verarbeitung in einer gesonderten und geschützten Umgebung, wirksame Kontroll- und Reaktionsmechanismen, die Einhaltung des Datenschutzrechts, technische und organisatorische Schutzmaßnahmen, eine umfassende Dokumentation und Protokollierung sowie Transparenz und Information über die Projekte erforderlich.

Als weitere innovationsfördernde Maßnahme soll unter bestimmten Voraussetzungen die Erprobung risikoreicher KI-Systeme (außerhalb von KI-Reallaboren) unter realen Bedingungen ermöglicht werden. Voraussetzung hierfür ist ein Testplan, der der zuständigen Aufsichtsbehörde vorgelegt und von dieser genehmigt werden muss. Entscheidet die Behörde nicht innerhalb von 30 Tagen über die Zulässigkeit der Erprobung, gilt der Plan als genehmigt. Die Möglichkeit, KI-Systeme mit hohem Risiko unter realen Bedingungen zu testen, kann jederzeit vor dem Inverkehrbringen oder der Inbetriebnahme des KI-Systems in Anspruch genommen werden, wobei die maximale Testdauer auf sechs Monate begrenzt ist. Um die möglichen Risiken der Tests zu begrenzen, müssen die Anbieter die Datensicherheit gewährleisten, qualifiziertes Personal zur Überwachung einsetzen und geeignete Maßnahmen zur Risikominimierung durchführen. Eine weitere zentrale Anforderung ist die Einholung einer informierten Einwilligung der von der Testung betroffenen Person. Vor Erteilung der jederzeit widerrufbaren Einwilligung muss die Testperson umfassend über die Art und die Ziele sowie über mögliche Nachteile der Tests informiert werden. Sollen hochriskante KI-Systeme unter realen Bedingungen getestet werden, ist zuvor eine Registrierung in einer zentralen EU-Datenbank erforderlich.

1.6 Durchsetzung und Sanktionen

Die Einhaltung der KI-Verordnung wird künftig behördlich überwacht. Hierzu werden auf nationaler Ebene entsprechende Aufsichtsbehörden eingerichtet bzw. bestehende Behörden mit der Marktüberwachung beauftragt. In Deutschland sind hierfür u. a. die Bundesnetzagentur, das Bundesamt für Sicherheit in der Informationstechnik und die Datenschutzbehörden im Gespräch. Anbieter von Hochrisiko-KI-Systemen müssen auf Verlangen der zuständigen Behörde die Konformität des KI-Systems mit den Anforderungen der Verordnung nachweisen können. Die Aufsichts-

behörde kann hierzu alle erforderlichen Auskünfte und Unterlagen verlangen. Dies schließt auch die Einsichtnahme in die automatisiert erstellten Protokolle des KI-Systems ein, soweit diese der Kontrolle des Anbieters unterliegen. Verstöße gegen die KI-Verordnung können mit Sanktionen wie Bußgeldern oder anderen Durchsetzungsmaßnahmen, einschließlich Verwarnungen, geahndet werden. Die Maßnahmen müssen „wirksam, verhältnismäßig und abschreckend" sein. Bei Verstößen gegen verbotene KI-Praktiken können Bußgelder in Höhe von bis zu 35 Millionen Euro oder sieben Prozent des gesamten weltweiten Jahresumsatzes verhängt werden. Bei Verstößen gegen die übrigen Anforderungen können Bußgelder in Höhe von 15 Millionen Euro oder drei Prozent des gesamten weltweiten Jahresumsatzes verhängt werden. Bei der Verhängung von Sanktionen gegen KMU ist deren wirtschaftliche Leistungsfähigkeit zu berücksichtigen.

1.7 Auswirkungen auf FuE-Projekte

Die KI-Verordnung enthält zahlreiche Vorgaben, die zukünftig Einfluss auf die Entwicklung und den Einsatz von KI-Systemen haben werden. Rechtsunsicherheiten für Forschungsprojekte und Unternehmen ergeben sich vor allem bei der Frage, ob es sich bei der zu entwickelnden Software oder dem Produkt um ein KI-System handelt. Der Begriff des KI-Systems wurde im Laufe des Gesetzgebungsverfahrens mehrfach präzisiert und orientiert sich nun an der OECD-Definition, die vor allem auf die Merkmale Autonomie und Inferenzfähigkeit von KI abstellt. Software oder Produkte, die unterhalb dieser Anforderungen operieren, sind keine KI-Systeme und unterliegen daher nicht den Vorgaben der Verordnung. Forschungsprojekte und Unternehmen sollten bei der Anwendung der Definition u. a. die Leitlinien beachten, die nach Verabschiedung der KI-Verordnung durch die EU-Kommission ausgearbeitet werden.

Handelt es sich bei der Software oder dem Produkt um ein KI-System, ist der Anwendungsbereich der KI-Verordnung grundsätzlich eröffnet. Ausgenommen sind lediglich KI-Systeme, die unter einer freien oder offenen Lizenz veröffentlicht werden, sowie KI-Systeme und -Modelle, die ausschließlich für Zwecke der wissenschaftlichen Forschung und Entwicklung erstellt und in Betrieb genommen werden, sofern diese nicht verboten oder mit einem hohen Risiko verbunden sind. Gleiches gilt für Forschungs-, Test- und Entwicklungstätigkeiten vor der Markteinführung oder Inbetriebnahme, sofern diese Aktivitäten nicht unter realen Einsatzbedingungen stattfinden. Auch diese Tätigkeiten sind von der Verordnung ausgenommen. Anbieter, die nicht aufgrund einer dieser Ausnahmen vom Anwendungsbereich der Verordnung ausgenommen sind, müssen ihr KI-System einer Risikoklassifizierung unterziehen. Geht von dem KI-System nur ein geringes Risiko aus, müssen nur Transparenzanforderungen umgesetzt werden. Für KI-Systeme mit minimalem Risiko bestehen keine rechtlichen Anforderungen. Die Anbieter solcher Systeme können sich jedoch freiwillig Verhaltenskodizes unterwerfen. Darüber hinaus wird sowohl von den Anbietern als auch von den Betreibern verlangt, dass ihr Personal ausreichend im Umgang mit KI-Systemen geschult ist.

Bei KI-Systemen mit hohem Risiko gestaltet sich die Risikoeinstufung komplexer. Anbieter von KI-Systemen im Sinne von Anhang I Abschnitt B (KI-System ist Produkt oder Sicherheitskomponente eines Produkts und unterliegt einer EU-Sicherheitsregulierung, siehe Abschnitt 1.3.2 , Fall 2) sind weitgehend von den Anforderungen der KI-Verordnung ausgenommen. Dennoch sollten Forschungsprojekte und Unternehmen, deren Produkte von den in Anhang I Abschnitt B genannten Rechtsakten betroffen sind, die Anforderungen der KI-Verordnung bei der Entwicklung ihrer Dienste

und Produkte berücksichtigen. Denn die bereichsspezifischen Sicherheitsregelungen werden durch die KI-Verordnung dahingehend angepasst, dass die Mindestanforderungen für Hochrisiko-KI-Systeme künftig im Rahmen der jeweiligen Rechtsakte zu beachten sind.

Anbieter von KI-Systemen, die gemäß Anhang I Abschnitt A als Systeme mit hohem Risiko eingestuft werden (siehe Abschnitt 1.3.2, Fall 1), müssen die Anforderungen der KI-Verordnung unmittelbar umsetzen. Berücksichtigt man, dass Produkte nach den dort genannten Rechtsakten bereits einer strengen Sicherheitsprüfung 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 Infrastrukturen, Bildung, Beschäftigung etc.) eingesetzt werden. Allerdings eröffnen sich auch hier Gestaltungsspielräume, die eine Befreiung von den Mindestanforderungen ermöglichen. Dies setzt jedoch eine intensive Vorprüfung voraus. FuE-Projekte sollten sich an den von der EU-Kommission bereitgestellten Leitlinien orientieren, die spätestens 18 Monate nach Inkrafttreten der Verordnung veröffentlicht werden und praktische Umsetzungsbeispiele für Hochrisiko- und Nicht-Hochrisiko-KI-Systeme enthalten.

Für Forschungsprojekte, aber auch für Akteure in Industriekooperationen kann die sehr schematische Einteilung in die Kategorien „Anbieter" und „Betreiber" zu Umsetzungsschwierigkeiten führen. Gerade große Forschungsprojekte mit einer Vielzahl von Kooperationspartnern zeichnen sich durch ein arbeitsteiliges Vorgehen aus. Häufig ist die Verantwortung für die Erforschung oder Entwicklung von KI-basierten Produkten oder Diensten auf eine Vielzahl von Akteuren und Institutionen verteilt. Mit Blick auf die zu erfüllenden Compliance-Vorgaben muss Klarheit darüber bestehen, wer in welchem Umfang für die Umsetzung der gesetzlichen Anforderungen verantwortlich ist. Die in der KI-Verordnung angelegten Sorgfalts- und Transparenzpflichten machen es erforderlich, dass die rechtlichen Anforderungen bereits in einer frühen Projektphase in den Entwicklungsprozess einfließen. Insgesamt müssen die betroffenen Akteure künftig mit einem höheren Aufwand für ihre KI-Compliance rechnen. Dies gilt insbesondere vor dem Hintergrund, dass bestimmte Anforderungen über den gesamten Lebenszyklus der KI einzuhalten sind.

Die Möglichkeit zur Teilnahme an KI-Reallaboren kann positive Impulse auf das Innovationsgeschehen haben. Das sich hieraus ergebende Potenzial für FuE-Projekte kann derzeit jedoch noch nicht genau abgeschätzt werden. Die Bedingungen für den Betrieb der KI-Reallabore einschließlich der Genehmigungskriterien stehen derzeit noch nicht fest, sondern müssen von der EU-Kommission im Rahmen von Durchführungsrechtsakten festgelegt werden. Zudem unterliegen die Einrichtung und der Betrieb der KI-Reallabore einer strengen behördlichen Aufsicht. Vor diesem Hintergrund sind Forschungsprojekte auf eine enge Kooperation mit den Aufsichtsbehörden angewiesen. Zudem kann die Möglichkeit, hochriskante KI-Systeme unter realen Bedingungen zu testen, zur Innovationsförderung beitragen, indem sie einen geschützten Rahmen für die Entwicklung, das Training und die Validierung neuer KI-Technologien schafft. Diese Maßnahmen ermöglichen es FuE-Projekten, ihre Systeme unter kontrollierten Bedingungen zu testen und wichtige Erkenntnisse zu gewinnen. Gleichzeitig stellen KI-Reallabore und die Möglichkeit zur Erprobung von KI-Systemen unter Realbedingungen keine pauschale Befreiung von den Anforderungen der KI-Verordnung dar. Sie können aber dazu beitragen, Innovationszyklen zu beschleunigen und das Risiko von Fehlentwicklungen zu verringern.

1.8 Umsetzungsstand

Die KI-Verordnung wurde am 12.07.2024 im Amtsblatt der Europäischen Union veröffentlicht und ist am 01.08.2024 in Kraft getreten. Die Vorschriften der KI-Verordnung sind damit nach einer Übergangsfrist von 24 Monaten ab dem 02.08.2026 unmittelbar anwendbar. Die Vorschriften für verbotene KI-Systeme gelten abweichend hiervon bereits ab dem 02.02.2025. Bei den Vorschriften für Hochrisiko-KI-Systeme ist eine längere Übergangszeit vorgesehen. Die Verpflichtungen für Hochrisiko-KI-Systeme müssen ab dem 02.08.2027 eingehalten werden. 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.

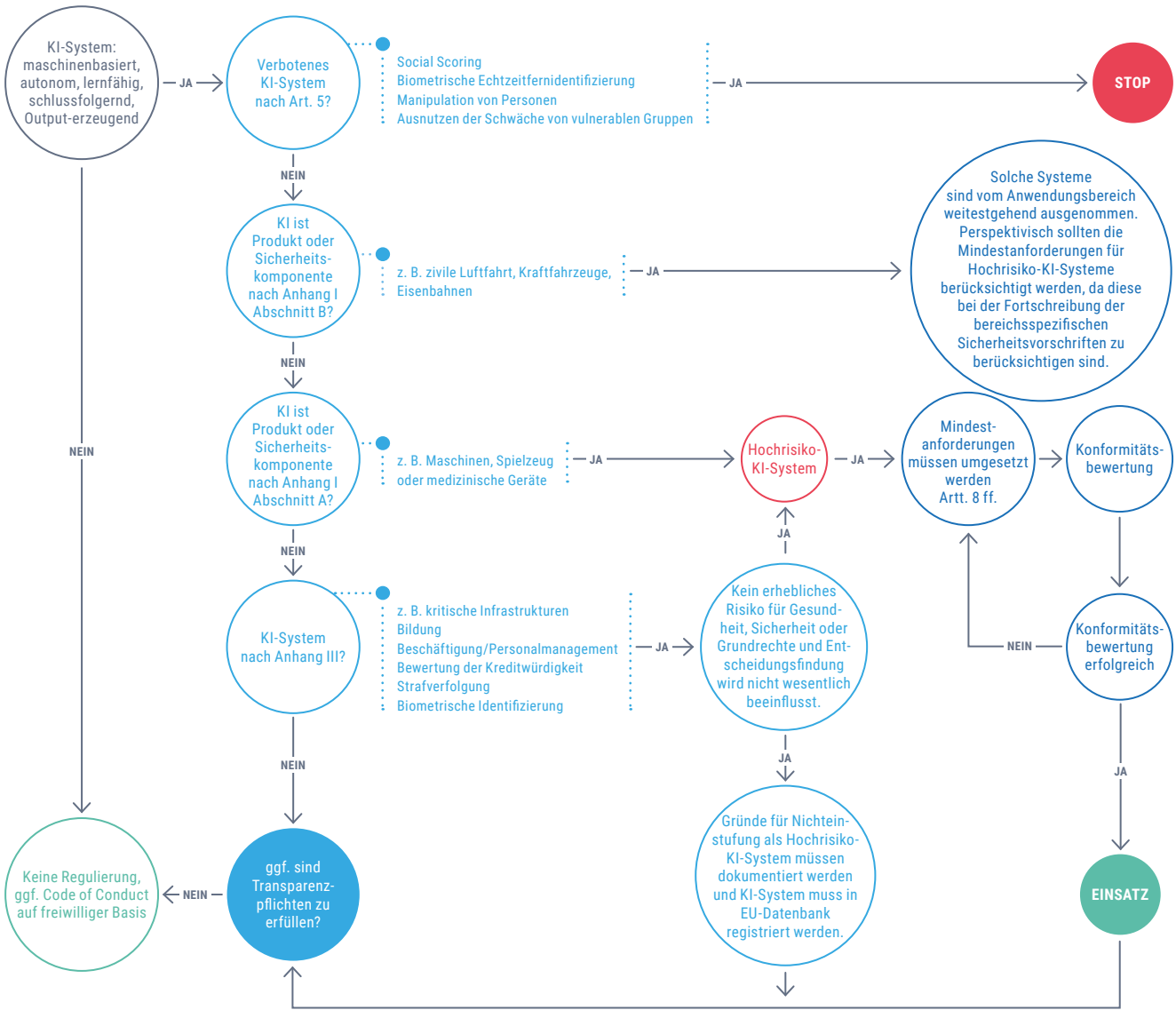


Abbildung 5: Das Prüfschema der KI-Verordnung

02

2 DATA GOVERNANCE ACT (DGA)

Die Europäische Kommission hat im Rahmen ihrer Datenstrategie den Entwurf einer Verordnung über eine europäische Daten-Governance[2] (Data Governance Act) vorgelegt. Mit dem Data Governance Act (DGA) sollen die Bedingungen für die gemeinsame Nutzung von Daten in der EU verbessert werden, indem ein harmonisierter Rechtsrahmen für den Datenaustausch geschaffen und grundlegende Anforderungen an die Daten-Governance festgelegt werden. Dadurch soll die Entwicklung eines einheitlichen digitalen Binnenmarkts und einer auf den Menschen ausgerichteten, vertrauenswürdigen und sicheren Datengesellschaft und -wirtschaft gefördert werden.

2.1 Anwendungsbereich und Adressatenkreis

Der DGA betrifft unterschiedliche Akteure und Anwendungsbereiche. Zunächst werden Regeln für den Umgang von besonders sensiblen Daten des öffentlichen Sektors festgelegt. Öffentliche Stellen wie Behörden, Kommunen oder öffentliche Körperschaften müssen künftig Vorgaben bei der Bereitstellung öffentlicher Datenbestände 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. Diese Regelungen gelten horizontal, d. h. übergreifend für alle Sektoren und Branchen. Schließlich soll der DGA die Etablierung sogenannter datenaltruistischer Organisationen fördern, die freiwillige „Datenspenden" für Zwecke 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 Erhöhung der Vertrauenswürdigkeit werden Anforderungen an die staatliche Anerkennung und die Eintragung in ein öffentliches Register für datenaltruistische Organisationen geschaffen.

Abbildung 6: Anwendungsbereich und Adressatenkreis des Data Governance Acts

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

2.2 Verbesserung der Verfügbarkeit von Daten öffentlicher Stellen

Die Erschließung von Datenbeständen des öffentlichen Sektors ist ein zentrales Anliegen der europäischen Datenstrategie. Mit der Open-Data-Richtlinie[3] wurde bereits 2019 ein rechtlicher Rahmen geschaffen, der den Zugang zu Daten des öffentlichen Sektors erleichtern soll. Die Vorgaben der Open-Data-Richtlinie wurden mit dem Datennutzungsgesetz (DNG) in nationales Recht umgesetzt. Darin ist unter anderem geregelt, dass Daten öffentlicher Stellen (z. B. Behörden, Kommunen, Einrichtungen des öffentlichen Rechts) kommerziell oder nicht-kommerziell weiterverwendet werden dürfen. Die Herausgabe besonders sensibler Daten war bisher nur eingeschränkt und unter Einhaltung verfahrenstechnischer und rechtlicher Vorgaben möglich. Erschwerend kam hinzu, dass die Anforderungen an die Nutzung dieser Daten in den einzelnen EU-Staaten sehr unterschiedlich geregelt waren. Mit dem DGA sollen nun EU-weit einheitliche Bedingungen für die Weiterverwendung sensibler Daten der öffentlichen Hand gelten. Öffentliche Stellen sind angehalten, den Schutz von sensiblen Daten zur gewährleisten, etwa indem personenbezogene Daten anonymisiert oder Geschäftsgeheimnisse nur in aggregierter oder aufbereiteter Form weitergeben werden dürfen. Außerdem muss die Bereitstellung über eine „sichere Verarbeitungsumgebung" erfolgen. Zum Schutz des Wettbewerbs ist zudem ein Verbot von Ausschließlichkeitsvereinbarungen vorgesehen. Das bedeutet, dass die Vergabe von exklusiven (Daten-)Lizenzen unter Ausschluss anderer Marktteilnehmer untersagt ist. Der öffentlichen Stelle steht es jedoch frei, für die Datennutzung Gebühren zu erheben. Für KMU, Start-ups und Bildungseinrichtungen kann die Gebühr ermäßigt werden. Die Bedingungen für die Weiterverwendung können in 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 die zentrale Stelle auch ermächtigen, selbst Datenzugangsentscheidungen zu treffen. Zur Erfüllung dieser Aufgaben ist die zentrale Stelle mit ausreichenden finanziellen, technischen und personellen Mitteln auszustatten. Um Nutzer bei der Suche nach relevanten Informationen über die bei den Behörden vorhandenen Daten zu unterstützen, sollen die Mitgliedstaaten darüber hinaus eine zentrale nationale Informationsstelle einrichten. In Deutschland ist vorgesehen, dass das Statistische Bundesamt als zentrale Informationsstelle fungiert. Abschließend ist festzuhalten, dass durch die Regelungen des DGA keine neuen Zugangsrechte zu öffentlichen Datenbeständen geschaffen werden. Es werden lediglich die Rahmenbedingungen für die Bereitstellung vorhandener, aber bisher nicht erschlossener Datenbestände vereinheitlicht.

2.3 Regulierung von Datenvermittlungsdiensten

Ein zentrales Element des DGA ist die Regulierung von Datenvermittlungsdiensten. Dabei handelt es sich um Anbieter, die als neutrale Intermediäre zwischen Dateninhabern und Datennutzern agieren und so eine gemeinsame Datennutzung ermöglichen. Datenvermittlungsdiensten wird eine Schlüsselrolle in der Datenwirtschaft zugeschrieben. Durch die Etablierung neutraler Vermittlungsinstanzen soll das Vertrauen in die gemeinsame Datennutzung gestärkt werden. Aus diesem Grund ist eine Monetarisierung der Daten durch den Datenvermittlungsdienst untersagt. Dies bedeutet, dass die vermittelten Daten weder weiterverkauft noch für die eigene Produktentwicklung

3 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.

verwendet werden. Zur Sicherstellung der Neutralität ist eine strukturelle und rechtliche Trennung der Datenvermittlung von anderen datenbezogenen Dienstleistungen erforderlich. 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[4]. Im Gegensatz dazu sind geschlossene Datenplattformen nicht als Datenvermittlungsdienste zu betrachten. Darunter sind Plattformen zu verstehen, auf denen Unternehmen Daten in nichtöffentlichen Gruppen austauschen, z. B. im Rahmen von Lieferanten- und Kundenbeziehungen. Anbieter, die Daten lediglich aggregieren, anreichern oder umwandeln und auf dieser Grundlage eigene Datenprodukte erstellen und vermarkten, gelten ebenfalls nicht als Datenvermittlungsdienste, da in diesen Fällen keine direkte Geschäftsbeziehung zwischen Dateninhabern und Datennutzern hergestellt wird. Cloud-Anbieter, Data-Sharing-Dienste oder Analysedienste fallen ebenfalls nicht in den Anwendungsbereich des DGA, da es sich hierbei lediglich um technische Werkzeuge für die gemeinsame Nutzung von Daten handelt, die nicht darauf abzielen, eine Geschäftsbeziehung zwischen den Inhabern und den Nutzern der Daten zu begründen.

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

4 Erwägungsgrund 28 des DGA.

Praxisbeispiel

Ein Unternehmen bietet digitale Karten und Geodatendienste über eine Plattform an. Neben der Bereitstellung eigener Kartendaten (2D-Geodarstellung von Straßennetzen, Wegen, Gebäuden, Strukturen, Orten, Landnutzung, Landbedeckung etc.) und Zusatzdiensten (z. B. Routenplanung) werden auch Daten Dritter, z. B. Verkehrsdaten von ÖPNV-Betreibern, über die Plattform angeboten. Geht man davon aus, dass die Daten von diesen Drittunternehmen unverändert nach dem Marktplatzprinzip verkauft werden, handelt das Unternehmen als Datenvermittlungsdienst im Sinne des DGA. Zukünftig wird es daher notwendig sein, die Bereiche der Datenvermittlung und des Angebots von datenbasierten Zusatzdiensten zu entflechten. Dazu muss die Datenvermittlung von einer eigenständigen juristischen Person erbracht werden. Zudem muss sich der Dienst vor Aufnahme seiner Tätigkeit registrieren lassen und eine Vielzahl von regulatorischen Anforderungen erfüllen (siehe Abschnitt 2.3).

Anders verhält es sich, wenn Datenbestände von Dritten aufgekauft werden, um sie anschließend zu aggregieren und anzureichern. Ein Beispiel wäre der Ankauf von Warenein- und -ausgangsdaten verschiedener Einzelhandelsunternehmen und die anschließende Aggregation und Aufbereitung zu globalen Marktdaten, z. B. zur Analyse, wann (z. B. saisonal oder anderweitig zyklisch), wie oft und welche Produkte im Einzelhandel gekauft und verkauft werden. Der Verkauf solcher veredelter Datensätze stellt keine Datenvermittlung dar (siehe Tabelle 1). Die gesetzlichen Anforderungen an Datenvermittlungsdienste müssen daher nicht eingehalten werden.

Der DGA enthält einen umfassenden Anforderungskatalog für Datenvermittlungsdienste, dessen Einhaltung behördlich überwacht werden soll. Um eine flächendeckende Erfassung der Anbieter von Datenvermittlungsdiensten zu gewährleisten, müssen sich diese vor Aufnahme ihrer Tätigkeit behördlich registrieren lassen. Erst nach erfolgter Anmeldung darf die Tätigkeit aufgenommen werden. Dabei sind eine Reihe von Vorgaben zu beachten. Im Mittelpunkt steht das **Neutralitätsgebot**. Es sieht eine strikte Trennung zwischen Datenvermittlung und Datennutzung vor. Anbieter dürfen hiernach nur als Vermittler fungieren und die Daten nicht für andere Zwecke nutzen. Unzulässig wären demnach z. B. datenbezogene Produkte oder Dienstleistungen, wie z. B. KI-gestützte Datenanalysen oder -dienstleistungen.

Lediglich Metadatenanalysen sind zulässig, wenn sie der Verbesserung des Datenvermittlungsdienstes dienen, z. B. Maßnahmen zur Betrugsprävention oder zur Gewährleistung der Cybersicherheit. Auch datenbezogene Angebote und Werkzeuge zur Erleichterung des Datenaustausches sind ein zulässiges Betätigungsfeld. Dazu gehören Dienste zur Speicherung, Pflege, Konvertierung, Anonymisierung und Pseudonymisierung von Daten. Diese datenbezogenen Dienste dürfen jedoch nur mit Zustimmung des Dateninhabers durchgeführt werden. Darüber hinaus ist der Datenvermittlungsdienst verpflichtet, die ihm übermittelten Daten unverändert weiterzuleiten. Eine Konvertierung 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 haben, der Konvertierung zu widersprechen („opt-out“).

Um die Neutralitätsanforderungen auch in der Organisationsstruktur des Anbieters zu verankern, ist zudem vorgesehen, dass Datenvermittlungsdienste von einer eigenen juristischen Person erbracht werden müssen. Eine wichtige Anforderung zur Stärkung der Wahlfreiheit von Dateninhabern und -nutzern ist die Anforderung, dass die Nutzung des Vermittlungsdienstes nicht von der Inanspruchnahme weiterer Dienste des Unternehmens abhängig gemacht werden darf. So wäre es beispielsweise untersagt, Preisnachlässe oder günstigere Konditionen nur dann zu gewähren, wenn zusätzliche Leistungen eines verbundenen Unternehmens gebucht werden (Hennemann und v. Ditfurth 2022, S. 1909). Als Ausdruck des Neutralitätsgedankens ist hinsichtlich des Zugangsverfahrens sicherzustellen, dass dieses fair, transparent und diskriminierungsfrei ist. So wäre es beispielsweise verboten, bestimmte Akteure ohne sachlichen Grund auszuschließen. Das Diskriminierungsverbot erstreckt sich auch auf die Preisbildung. Damit soll eine Benachteiligung durch die Preisgestaltung ausgeschlossen werden. Gleichzeitig verlangt das Transparenzgebot, dass die Zugangsbedingungen klar und verständlich kommuniziert werden.

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, unter denen der Datennutzer andere kommerzielle Dienste des Anbieters in Anspruch nehmen muss
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	Unfaire, intransparente oder diskriminierende Zugangsbedingungen einschließlich der Preisgestaltung
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 für die Gesellschaft von großem Interesse. Um ihr Potenzial besser nutzen zu können, müssen ausreichende Datenmengen zur Verfügung stehen. Ziel der DGA ist es, die Voraussetzungen für die Generierung dieser Datenmengen zu schaffen, u. a. durch die Förderung von **Datenaltruismus**. Darunter versteht man die freiwillige gemeinsame Nutzung von Daten, die der Dateninhaber ohne Erhalt einer Gegenleistung (altruistisch) zur Förderung von Zielen des Allgemeininteresses zur Verfügung stellt. Solche im öffentlichen Interesse liegenden Ziele sind die Gesundheitsversorgung, die Bekämpfung des Klimawandels, die Verbesserung der Mobilität oder die wissenschaftliche Forschung. Der DGA soll die Gründung von datenaltruistischen Organisationen erleichtern. Sie sollen sich beispielsweise in ein öffentliches Register eintragen lassen können, sofern sie über eine eigene Rechtspersönlichkeit verfügen und Ziele von allgemeinem Interesse verfolgen. Um ihre Unabhängigkeit zu wahren, dürfen sie keinen Erwerbszweck verfolgen und müssen sicherstellen, dass die altruistische Tätigkeit strukturell von anderen Tätigkeiten 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, wird die Europäische Kommission einen Vorschlag für ein europäisches Einwilligungsformular erarbeiten. Dieses soll modular aufgebaut sein, so dass es an bestimmte Sektoren und Zwecke angepasst werden kann. Damit datenaltruistische Organisationen leicht als solche erkannt werden können, soll auch ein EU-weit einheitliches Logo eingeführt werden. Das gemeinsame Logo wird mit einem QR-Code versehen, der auf das öffentliche EU-Register der anerkannten datenaltruistischen Organisationen verweist.

2.5 Durchsetzung und Sanktionen

Nach Art. 13 DGA sind die nationalen Behörden für das Anmeldeverfahren für Datenvermittlungsdienste zuständig und befugt, von den Anbietern von Datenvermittlungsdiensten alle erforderlichen Informationen zu verlangen, um die Einhaltung der Anforderungen zu überprüfen, die Durchführung bestimmter Maßnahmen zu überwachen und Sanktionen zu verhängen. Darüber hinaus sind Behörden zu benennen, die für die Registrierung von datenaltruistischen Organisationen zuständig sind und die Einhaltung der entsprechenden Vorschriften überwachen. Darüber hinaus sollen die EU-Mitgliedstaaten Regelungen über Sanktionen bei Verstößen gegen die Mitteilungspflichten von Datenvermittlungsdiensten, über die Voraussetzungen für die Erbringung von Datenvermittlungsdiensten sowie über die Voraussetzungen für die Registrierung als anerkannte Datenvermittlungsstelle treffen. Gegenüber Datenvermittlungsdiensten oder datenaltruistischen Organisationen, die in Zukunft gegen die Bestimmungen des DGA verstoßen, können behördliche Maßnahmen ergriffen werden. Wie und in welchem Umfang Sanktionen zu verhängen sind, ist nicht festgelegt. Es wird lediglich bestimmt, dass die Maßnahmen wirksam, verhältnismäßig und abschreckend sein müssen. Denkbar ist daher z. B. die Verhängung von Bußgeldern, wobei der DGA – im Gegensatz zu den anderen Rechtsakten – keinen konkreten Bußgeldrahmen vorgibt. Das derzeit im Gesetzgebungsverfahren befindliche Gesetz zur Durchführung der EU-Verordnung über europäische Daten-Governance sieht die Verhängung von Zwangsgeldern in Höhe von bis zu 25.000 Euro vor. Als zuständige Aufsichtsbehörde für die Überwachung von Datenvermittlungsdiensten und datenaltruistischen Organisationen ist die Bundesnetzagentur vorgesehen.

2.6 Auswirkungen auf FuE-Projekte

Die Regelungen zur Weiterverwendung von Daten können dazu beitragen, Informationen der öffentlichen Verwaltung in Zukunft leichter verfügbar zu machen. Gleichzeitig werden jedoch keine neuen Zugangsrechte geschaffen, sondern lediglich die Bedingungen vereinheitlicht, unter denen eine Weiterverwendung stattfinden kann. Inwieweit sich dadurch die Dichte der nutzbaren Datenbestände erhöht, kann derzeit noch nicht abschließend beurteilt werden. Dennoch sind die neuen Regelungen aus Sicht von Forschungsprojekten, aber auch von Unternehmen und Start-ups positiv zu bewerten. Denn nun gelten EU-weit einheitliche Standards und Verfahren für den Zugang zu besonders sensiblen Daten der öffentlichen Hand. Zudem kann die im DGA vorgesehene zentrale Informationsstelle zur Vereinfachung des Antragsverfahrens beitragen. Die zu erstellende zentrale Bestandsliste kann darüber hinaus das Auffinden von Daten erleichtern. Ungelöst bleiben jedoch praktische Probleme, insbesondere auf Seiten der bereitstellenden Institutionen: etwa die Frage, wann Daten als anonymisiert gelten oder ob Gebühren für die Bereitstellung von Daten verhältnismäßig sind. Die datenwirtschaftlichen Impulse des DGA könnten hinter den Erwartungen zurückbleiben, wenn die öffentliche Hand die Vorgaben in der Praxis nicht umsetzen kann.

Der DGA wird darüber hinaus ein verbindliches Leitbild für die zukünftige Governance von Datenvermittlungsdiensten vorgeben. Der neue Rechtsrahmen wird erhebliche Auswirkungen auf die Ausgestaltung und Organisationsform von Datenintermediären haben. Betroffen sind vor allem offene Plattformen wie Datenmarktplätze, Datendrehscheiben oder Datenplattformen für spezifische Branchenökosysteme. Das Neutralitätsgebot der DGA bedeutet, dass diese Anbieter die über die Plattform bereitgestellten Daten nicht monetarisieren dürfen. Anbieter von Datenvermittlungsdiensten müssen daher ihr Geschäfts- und Betriebsmodell anpassen und die strukturelle Trennung von Datenvermittlungs- und Datennutzungsdiensten sicherstellen. Dies setzt u. a. voraus, dass der Datenvermittlungsdienst von einer separaten juristischen Person erbracht wird. Forschungs- und Entwicklungsprojekte müssen bereits in einer frühen Projektphase ein Verständnis für die Rollenverteilung der jeweiligen Akteure innerhalb des Datenökosystems entwickeln. Dabei ist sicherzustellen, dass datenbasierte Zusatzdienste, wie KI- oder Big-Data-Analysen, nicht von der Vermittlungsplattform selbst angeboten werden. Die Umsetzung der gesetzlichen Anforderungen bedeutet für Forschungsprojekte einen erhöhten Aufwand. Im Hinblick auf die Phase nach Projektende, in der es insbesondere um den Weiterbetrieb von Plattformen geht, ist zu berücksichtigen, dass die Beschränkung auf die Datenvermittlung den Spielraum für tragfähige Geschäftsmodelle stark einschränken kann.

Diesen Einschränkungen können jedoch auch Vorteile gegenüberstehen. Die Etablierung neutraler Vermittlungsinstanzen kann auch zu mehr Vertrauen zwischen den Akteuren der Datenwirtschaft führen. Ob die vom Verordnungsgeber intendierte Etablierung von Datenvermittlungsdiensten tatsächlich eintritt, ist derzeit nicht absehbar.

Abbildung 7: Auswirkungen des DGA auf Datenintermediäre

In Zukunft könnte die Förderung von datenaltruistischen Organisationen zur Erschließung neuer Datenbestände führen. Davon könnten nichtkommerzielle Datenplattformen profitieren, die gemeinwohlorientierte Ziele verfolgen. Durch die Bereitstellung eines einheitlichen Einwilligungsformulars könnten Unsicherheiten über die Wirksamkeit einer Einwilligung reduziert werden. Inwieweit dieser Ansatz zur Förderung von Datenaltruismus beiträgt und inwieweit dadurch das Vertrauen in die Bereitstellung von Daten erhöht wird, kann derzeit nicht abgeschätzt werden.

2.7 Umsetzungsstand

Der DGA ist am 23.06.2022 in Kraft getreten und gilt seit dem 24.09.2023 unmittelbar in der gesamten EU. Für Anbieter, die am 23.06.2022 bereits Datenvermittlungsdienste erbracht haben, gilt eine Übergangsfrist. Sie müssen die Verpflichtungen der Verordnung erst ab dem 24.09.2025 erfüllen. Das nationale Ausführungsgesetz zum DGA (Daten-Governance-Gesetz) befindet sich derzeit in der Verabschiedung. Darin werden insbesondere Fragen der Zuständigkeiten sowie der Befugnisse und Sanktionsinstrumente der Aufsichtsbehörden geregelt.

03

3 DATA ACT (DA)

Als zweite Säule der europäischen Datenstrategie wurde mit der Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung[5] (Data Act) ein weiteres datenwirtschaftliches Regulierungsvorhaben auf den Weg gebracht. Der Data Act schafft einen sektorübergreifenden Governance-Rahmen für die gemeinsame Nutzung von Daten und soll künftig festlegen, wer – neben dem Hersteller von Produkten – unter welchen Bedingungen und auf welcher Grundlage auf Daten zugreifen darf. Hintergrund des Legislativvorschlags ist die Annahme, dass ein Großteil der in Maschinen und Produkten enthaltenen Daten aufgrund fehlender Zugriffsmöglichkeiten und -rechte nicht wirtschaftlich verwertbar ist.[6] Der Data Act soll dem entgegenwirken und bestehende Hindernisse für die gemeinsame Nutzung von Daten zum Vorteil von Unternehmen, Verbraucherinnen und Verbrauchern sowie der öffentlichen Hand abbauen und neue Impulse für datengetriebene Innovationen setzen.

3.1 Anwendungsbereich

Der Data Act richtet sich in erster Linie an Hersteller, die ihre Produkte innerhalb der EU in Verkehr bringen. Erfasst werden Produkte, die während ihres Betriebs Daten über ihre Nutzung oder ihre Umwelt erzeugen und in der Lage sind, diese Daten elektronisch zu übertragen. Dies sind typischerweise vernetzte Produkte wie Maschinen, Fahrzeuge, Haushaltsgeräte oder elektronische Konsumgüter. Neben den Herstellern fallen auch die Anbieter so genannter „verbundener Dienste" in den Anwendungsbereich der Verordnung. Dabei handelt es sich um digitale Dienste, die integraler Bestandteil eines Produkts sind und ohne die das Produkt nicht funktionieren würde. Da sie die technisch-faktische Hoheit über die generierten Daten haben, müssen sie darüber hinaus weitere Anforderungen erfüllen. Dies schließt die Verpflichtung ein, den Nutzern des Produkts Zugang zu ihren Daten zu gewähren. Ferner besteht die Verpflichtung, auf Antrag des Nutzers Dritten Zugang zu den Daten zu gewähren. Bei diesen Datenempfängern handelt es sich typischerweise um Akteure, die im Auftrag des Nutzers 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 z. B. Autowerkstätten oder Wartungsdienste.

5 Verordnung (EU) 2023/2854 des Europäischen Parlaments und des Rates über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz), https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202302854.

6 Eine Ausnahme gilt für personenbezogene Daten, wo betroffene Personen nach den Vorschriften der EU-Datenschutz-Grundverordnung ein Recht auf Auskunft und Datenportabilität haben.

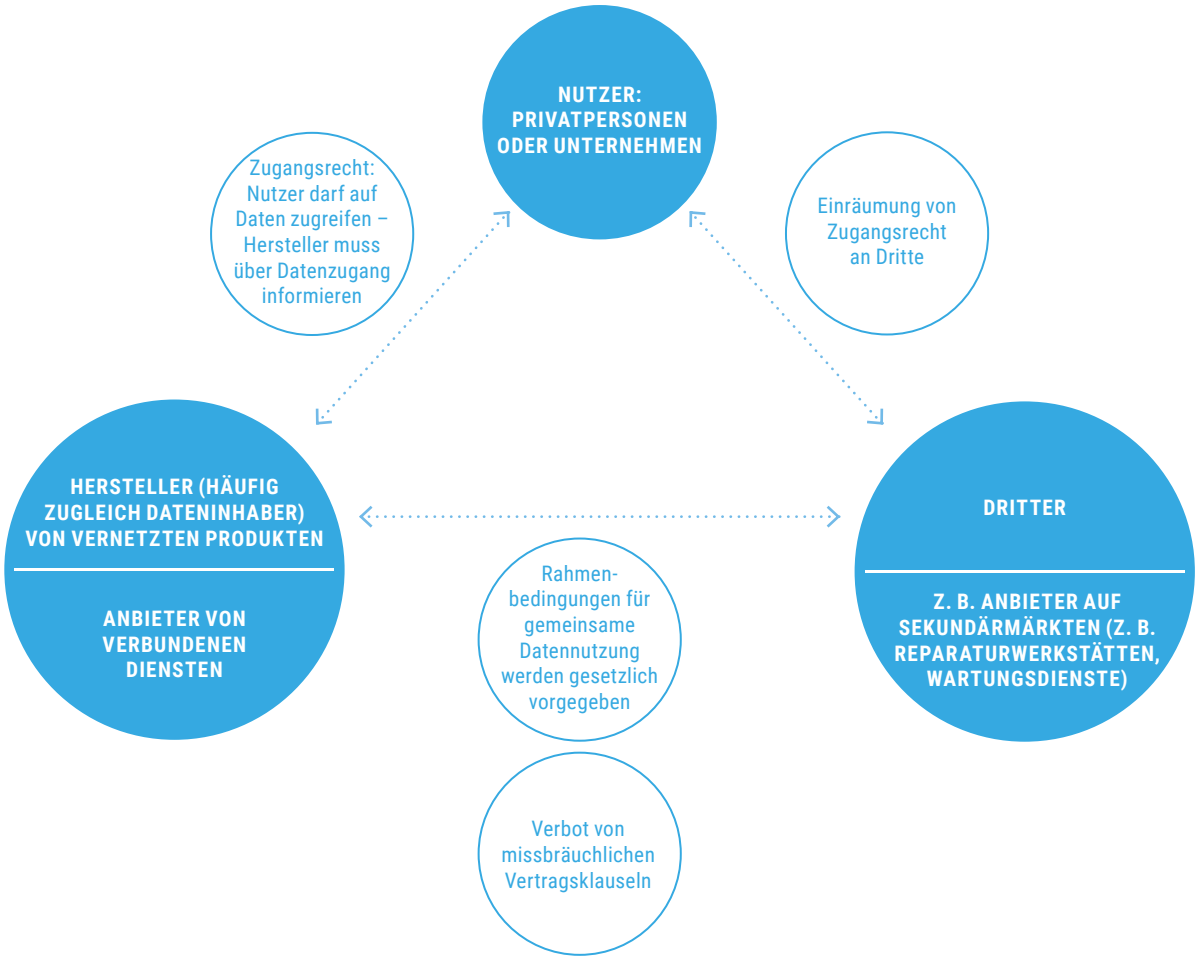


Abbildung 8: Übersicht zu den Beziehungen und Ansprüchen der Akteure

3.2 Pflicht zur Zugänglichmachung von Nutzungsdaten

Der Data Act formuliert zunächst Pflichten im Hinblick auf die **Produktgestaltung**. Voraussetzung für eine datenbasierte Wertschöpfung ist, dass die dafür notwendigen Daten auch technisch verfügbar sind. Künftig besteht die Verpflichtung, Produkte so zu gestalten und herzustellen, dass die bei ihrer Nutzung anfallenden Daten für die Nutzer standardmäßig einfach, sicher und unmittelbar zugänglich sind **(Accessibility by Design and by Default)**. Um die Möglichkeiten der Datenverwendung erkennbar zu machen, soll der Hersteller künftig zudem verpflichtet werden, gegenüber dem Käufer, Mieter oder Leasingnehmer eines Produkts bestimmte Transparenz- und Informationspflichten zu erfüllen. Hierzu gehört etwa die Offenlegung über die Art und den Umfang der durch die Nutzung entstehenden Daten und wie der Nutzer auf diese Daten zugreifen kann.

3.3 Recht des Nutzers auf Datenzugang

Um Nutzern den Zugang zu den von ihnen erzeugten Daten zu ermöglichen, wurde das Recht auf Datenzugang geschaffen. Dieses Recht besteht gegenüber dem Dateninhaber, d. h. gegenüber demjenigen, der aufgrund der Kontrolle über die technische Gestaltung des Produkts in der Lage ist, bestimmte Daten zur Verfügung zu stellen. Auf Verlangen des Nutzers muss der Dateninhaber (in der Regel der Hersteller) die bei der Nutzung eines Produkts erzeugten Daten unverzüglich, kostenlos und gegebenenfalls kontinuierlich und in Echtzeit zur Verfügung stellen. Kleinst- oder Kleinunternehmen[7] sind von der Pflicht zur Datenbereitstellung befreit. Zum Schutz der Interessen des Dateninhabers sind Einschränkungen des Datenzugangsrechts vorgesehen. So dürfen Geschäftsgeheimnisse des Dateninhabers nur offenbart werden, wenn Maßnahmen getroffen wurden, um die Vertraulichkeit der Geschäftsgeheimnisse insbesondere gegenüber Dritten zu wahren. Der Verordnungsgeber scheint dabei den Abschluss von Vertraulichkeitsvereinbarungen im Auge zu haben (Hennemann und Steinrötter 2022, S. 1484). Scheitert eine entsprechende Vereinbarung oder setzt der Nutzer die vertraglich geschuldeten Maßnahmen nicht um, darf die Datenbereitstellung verweigert werden. Gleiches gilt, wenn der Dateninhaber nachweisen kann, dass trotz der getroffenen Maßnahmen der Eintritt eines schweren wirtschaftlichen Schadens wahrscheinlich ist. Die Umstände der Verweigerung müssen hinreichend begründet werden. Es besteht auch die Verpflichtung, die zuständige Behörde über die Verweigerung zu informieren. Der Nutzer kann sich gegen die Verweigerung der Datenbereitstellung wehren und den Rechtsweg beschreiten. Alternativ kann er bei der zuständigen Behörde Beschwerde einlegen oder die zuständige Streitbeilegungsstelle anrufen.

Als weitere Einschränkung ist es dem Nutzer untersagt, mit den erhaltenen Daten eigene Produkte zu entwickeln, die mit den Produkten des Dateninhabers konkurrieren. 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 Datenverarbeitung ist nur dann zulässig, wenn eine entsprechende vertragliche Vereinbarung zwischen Dateninhaber und Datennutzer besteht, die dies erlaubt. Dazu ist es notwendig, die Zustimmung des Nutzers zur Datennutzung einzuholen, beispielsweise wenn die Daten zur Weiterentwicklung eigener Produkte verwendet werden sollen.

Das Zugangsrecht bezieht sich auf alle Daten, die bei der Nutzung des Produkts anfallen. Dies umfasst sowohl vom Nutzer gezielt erzeugte Daten, als auch Daten, die als Nebenprodukt von Nutzeraktionen entstehen (z. B. Diagnosedaten). Erfasst werden auch Daten, die ohne Interaktion des Nutzers anfallen, z. B. wenn sich das Produkt im Standby-Modus befindet oder ausgeschaltet ist. Ebenfalls erfasst sind Umgebungsdaten, die durch die Nutzung 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.

7 nach Art. 2 der Empfehlung 2003/361/EG sind Kleinstunternehmen Unternehmen mit weniger als 10 Mitarbeitern und einem Jahresumsatz oder einer Jahresbilanzsumme von höchstens 2 Mio. EUR. Kleine Unternehmen sind Unternehmen, die weniger als 50 Mitarbeiter und einen Jahresumsatz oder eine Jahresbilanzsumme von höchstens 10 Mio. EUR haben. Mittlere Unternehmen sind Unternehmen, die weniger als 250 Mitarbeiter und einen Jahresumsatz von höchstens 50 Mio. EUR oder eine Jahresbilanzsumme von höchstens 43 Mio. EUR haben.

3.4 Recht auf Weitergabe von Daten an Dritte

Auf Verlangen des Nutzers hat der Dateninhaber die bei der Nutzung eines Produkts anfallenden Daten auch einem Dritten zur Verfügung zu stellen, wobei die gleichen Anforderungen gelten wie für die Bereitstellung der Daten an den Nutzer selbst. Die Herausgabe hat insbesondere unverzüglich und für den Nutzer unentgeltlich zu erfolgen. Einschränkungen bestehen für große Plattformdienste. Diese sind keine zulässigen Datenempfänger, sofern sie aufgrund ihrer Marktstellung als Gatekeeper im Sinne des Digital Markets Acts (DMA) benannt wurden (siehe Kapitel 5). Die Bereitstellung von Daten an diese Plattformen kann daher vom Dateninhaber verweigert werden.

Der Dateninhaber kann das Weitergabeverlangen des Nutzers nicht pauschal mit Verweis auf den Geschäftsgeheimnisschutz ablehnen. **Geschäftsgeheimnisse** müssen Dritten aber nur insoweit offengelegt werden, als dies für den zwischen dem Nutzer 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. Wird keine Einigung über die erforderlichen Maßnahmen erzielt oder setzt der Dritte diese nicht um, kann der Dateninhaber die Datenübermittlung verweigern oder aussetzen. Auch in diesem Fall ist die Verweigerung der Datenübermittlung zu begründen und der zuständigen Behörde mitzuteilen. Eine Ablehnung ist auch dann zulässig, wenn der Dateninhaber nachweisen kann, dass trotz der getroffenen Maßnahmen ein schwerer wirtschaftlicher Schaden wahrscheinlich ist. Auch in diesem Fall sind die tatsächlichen Umstände des schweren wirtschaftlichen Schadens zu begründen und der zuständigen Behörde mitzuteilen. Dem Dateninhaber steht es frei, die Entscheidung gerichtlich überprüfen zu lassen oder Beschwerde bei der zuständigen Behörde einzulegen.

Zum Schutz der Interessen des Dateninhabers darf der Datenempfänger die ihm übermittelten Daten seinerseits nicht nach Belieben verwenden. So ist es ihm beispielsweise untersagt, die erhaltenen Daten für die Entwicklung von Konkurrenzprodukten zu verwenden oder an zentrale Plattformdienste (Gatekeeper im Sinne des Digital Markets Act) weiterzuleiten. Zur Wahrung der Interessen des Nutzers ist es dem Dateninhaber darüber hinaus untersagt, die erhaltenen Daten zum Zwecke der Profilbildung zu verwenden.

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 fordern, etwa in Form einer Vergütung. Dieses Entgelt muss jedoch angemessen sein. Darüber hinaus sind Vorgaben zu technischen Schutzmaßnahmen zulässig. Vorgesehen ist auch die Einrichtung von Schlichtungsstellen, die unter anderem die Aufgabe haben, die Vertragsbedingungen auf ihre Fairness, Angemessenheit und Diskriminierungsfreiheit zu überprüfen.

Darüber hinaus sieht der Data Act ein Verbot missbräuchlicher Vertragsklauseln vor, die ein Unternehmen einem anderen einseitig auferlegt. Solche Klauseln sind für das benachteiligte

Unternehmen nicht bindend, wenn sie als missbräuchlich gelten, d. h., wenn sie erheblich von der guten Handelspraxis abweichen oder gegen Treu und Glauben verstoßen. Vertragsklauseln über den Zugang und die Nutzung von Daten unterliegen damit einer Inhaltskontrolle, die mit der AGB-Klauselkontrolle des BGB vergleichbar ist (Klink-Straub und Straub 2022). In diesem Zusammenhang werden beispielhaft verschiedene Konstellationen aufgezählt, die eine Missbräuchlichkeit vermuten lassen. Zu beanstanden sind insbesondere Klauseln, die eine unverhältnismäßige Haftungsfreistellung vorsehen oder der benachteiligten Partei wesentliche Rechtsbehelfe für den Fall der Nichterfüllung von Vertragspflichten vorenthalten. Darüber hinaus enthält der Data Act einen weiteren, breiter gefassten Katalog von Missbrauchstatbeständen, die sich auf spezifische Vertragskonstellationen beziehen. Dazu gehören die Verhinderung der Nutzung der eigenen Daten durch den Vertragspartner oder die Möglichkeit, den Vertrag innerhalb einer angemessenen Frist zu kündigen.

Um Vertragsverhandlungen über den Zugang zu Daten und deren Nutzung zu erleichtern, wird die Europäische Kommission bis zum 12. September 2025 unverbindliche Muster- und Standardvertragsklauseln zur Verfügung stellen. Diese Klauseln werden auch Bedingungen für eine angemessene Gegenleistung und den Schutz von Geschäftsgeheimnissen enthalten. Damit sollen Unternehmen bei der Aushandlung fairer und diskriminierungsfreier Vertragsbedingungen unterstützt werden.

3.6 Regelungen zugunsten von KMU und Forschungseinrichtungen

Der Data Act enthält an verschiedenen Stellen Regelungen zum Schutz schwächerer Marktteilnehmer. So sind Klein- und Kleinstunternehmen[8] als Dateninhaber von den oben genannten Pflichten zur Datenbereitstellung befreit. Darüber hinaus stellt das Verbot missbräuchlicher Vertragsklauseln ein Abwehrinstrument für kleine und mittlere Unternehmen dar, die in vielen Vertragssituationen tendenziell benachteiligt werden. Damit soll durch Einschränkung der Vertragsfreiheit sichergestellt werden, dass auch schwächere Vertragsparteien zu fairen Bedingungen an der datenbasierten Wertschöpfung partizipieren können. Klein- und Kleinstunternehmen werden auch im Hinblick auf die Vergütung, die der Dateninhaber für die Bereitstellung von Daten an Dritte vorsehen kann, privilegiert. Grundsätzlich gilt, dass jedes Entgelt, das für die Bereitstellung von Daten vereinbart wird, nichtdiskriminierend und angemessen sein muss. Eine Gewinnmarge zugunsten des Dateninhabers ist jedoch zulässig. Der Dateninhaber darf bei der Berechnung der Gegenleistung insbesondere die angefallenen Kosten für die Bereitstellung der Daten und gegebenenfalls Investitionen in die Erhebung und Generierung der Daten berücksichtigen. Für KMU und gemeinnützige Forschungseinrichtungen gilt eine Kostenobergrenze. Danach darf das Entgelt die tatsächlichen Kosten des Dateninhabers für die Bereitstellung der Daten nicht übersteigen. Dies bedeutet, dass nur die tatsächlichen Kosten der Datenbereitstellung, wie z. B. die Formatierung und Speicherung der Daten sowie deren elektronische Übermittlung, in Rechnung gestellt werden dürfen. Durch die Begrenzung der Höhe des Entgelts können insbesondere kleinere Unternehmen sowie Forschungseinrichtungen profitieren und leichteren Zugang zu den benötigten Daten erhalten.

8 nach Art. 2 der Empfehlung 2003/361/EG sind Kleinstunternehmen Unternehmen mit weniger als 10 Mitarbeitern und einem Jahresumsatz oder einer Jahresbilanzsumme von höchstens 2 Mio. EUR. Kleine Unternehmen sind Unternehmen, die weniger als 50 Mitarbeiter und einen Jahresumsatz oder eine Jahresbilanzsumme von höchstens 10 Mio. EUR haben. Mittlere Unternehmen sind Unternehmen, die weniger als 250 Mitarbeiter und einen Jahresumsatz von höchstens 50 Mio. EUR oder eine Jahresbilanzsumme von höchstens 43 Mio. EUR haben.

3.7 Wechsel zwischen Cloud-Anbietern

Der Data Act enthält auch Regelungen, die den Wechsel zwischen Cloud-Anbietern erleichtern sollen. Konkret sollen gewerbliche, technische, vertragliche und organisatorische Hürden abgebaut werden, die einen Wechsel erschweren oder verhindern. Vorgesehen sind beispielsweise Vorgaben zu den vertraglichen Rahmenbedingungen, wie eine maximale Kündigungsfrist von 30 Tagen oder die Möglichkeit, Daten von einem Anbieter auf einen anderen zu übertragen. In diesem Fall müssen die Anbieter von Cloud-Diensten die Kunden bei der Umstellung unterstützen und die uneingeschränkte Kontinuität der Bereitstellung der betreffenden Funktionen oder Dienste gewährleisten. In diesem Zusammenhang sollen auch Entgelte für einen beantragten Wechsel abgeschafft bzw. für bestimmte Transaktionen auf die Grenzkosten beschränkt werden. Darüber hinaus werden technische Vorgaben zur Verwendung offener Schnittstellen sowie zur Kompatibilität mit offenen Interoperabilitätsspezifikationen bzw. europäischen Interoperabilitätsnormen gefordert.

3.8 Datenbereitstellung an öffentliche Stellen

Darüber hinaus ist auch eine Datenübermittlungspflicht an öffentliche Stellen oder Einrichtungen der EU vorgesehen. Dies ist jedoch nur in außergewöhnlichen Notstandssituationen (z. B. Naturkatastrophen, Notlagen im Bereich der öffentlichen Gesundheit) möglich und zudem zeitlich befristet. Qualitativ muss die Notlage so gravierend sein, dass schwerwiegende und dauerhafte Folgen für die Lebensbedingungen oder die wirtschaftliche Stabilität zu erwarten sind. Das Herausverlangen von Daten durch öffentliche Stellen ist nur zulässig, wenn die Daten zur Bewältigung eines öffentlichen Notstandes tatsächlich erforderlich sind und dem Staat auch keine anderen Datenquellen zur Verfügung stehen. Im Falle eines öffentlichen Notstandes sind staatliche Einrichtungen auch berechtigt, die erhaltenen Daten an Forschungseinrichtungen weiterzugeben. Allerdings sind nur gemeinnützige oder im öffentlichen Interesse handelnde Forschungsorganisationen berechtigt. Diese dürfen zudem nicht unter dem bestimmenden Einfluss von gewerblichen Unternehmen stehen.

3.9 Durchsetzung und Sanktionen

Die Aufsicht und Durchsetzung der Bestimmungen der Verordnung erfolgt auf nationaler Ebene. Zu diesem Zweck benennt jeder Mitgliedstaat eine oder mehrere zuständige Behörden, deren Aufgabe es unter anderem ist, über den Inhalt und die Verpflichtungen der Verordnung zu informieren. Die zuständige Behörde bearbeitet auch Beschwerden über mögliche Verstöße und ist befugt, Sanktionen zu verhängen, die auch Zwangsgelder und Geldbußen umfassen können. Die Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein. Geldbußen können bis zu 20 Millionen Euro oder vier Prozent des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs betragen.

3.10 Auswirkungen auf FuE-Projekte

Dem Data Act liegt ein horizontaler Regelungsansatz zugrunde. Das bedeutet, dass er Regeln für die gemeinsame Nutzung von Daten festlegt, die sektorübergreifend und unabhängig von einer bestimmten Branche gelten. Das Regelwerk wirkt sich in erster Linie auf Forschungsprojekte und Unternehmen aus, die auf die Entwicklung vernetzter Produkte ausgerichtet sind. Bereits in der Entwicklungsphase eines Produkts muss darauf geachtet werden, dass die anfallenden Nutzungsdaten standardmäßig einfach, sicher und direkt zugänglich sind. Gleiches gilt für die Gestaltung von verbundenen Diensten, d. h. Diensten, die mit vernetzten Produkten interagieren und integraler Bestandteil dieser Produkte sind. Plattformen, Schnittstellen oder Benutzeroberflächen müssen daher auch das Prinzip „Accessibility by Default" umsetzen. In Forschungsprojekten erfordert dies eine enge Abstimmung zwischen den Akteuren. Dies betrifft sowohl die Entwicklung des physischen Produkts selbst als auch die darauf aufbauende Software. Darüber hinaus muss – nicht zuletzt im Hinblick auf die zu erfüllenden Informationspflichten – Klarheit darüber bestehen, welche Daten als „Nutzungsdaten" der Bereitstellungspflicht unterliegen. Weiterhin müssen Vorkehrungen getroffen werden, wie der Nutzer über die ihm zur Verfügung stehenden Daten und Rechte informiert wird. Schließlich ist zu beachten, dass der Hersteller die generierten Nutzungsdaten nur dann für eigene Zwecke verwenden darf, wenn er zuvor die Zustimmung des Nutzers eingeholt hat.

Die im Data Act angelegten Akteursbeziehungen zwischen Dateninhaber, Nutzer und Datenempfänger können zu Umsetzungsschwierigkeiten führen. Diese schematische Dreiecksbeziehung wird der Aufgaben- und Arbeitsteilung in FuE-Projekten, insbesondere in komplexen Datenökosystemen häufig nicht gerecht. Die Akteure in Forschungsprojekten, aber auch in Industriekooperationen müssen sich künftig stärker über die jeweiligen Rollen und die damit verbundenen Verantwortlichkeiten abstimmen. Zudem wird der Schutz von Geschäftsgeheimnissen der Dateninhaber im Data Act nicht als vorrangiges Ziel gesehen, sondern mit den Interessen der anderen Akteure abgewogen. Insbesondere dürfen Zugangsanfragen nicht pauschal mit dem Hinweis auf die Sensibilität von Unternehmensdaten abgelehnt werden. In FuE-Projekten, aber auch im unternehmerischen Kontext, wird daher in Zukunft verstärkt darauf zu achten sein, welche technischen und rechtlichen Schutzmaßnahmen den Datenempfängern auferlegt werden, um die Vertraulichkeit der zur Verfügung gestellten Daten zu gewährleisten.

Forschungsprojekte und Unternehmen müssen sicherstellen, dass Produkte so gestaltet sind, dass die Nutzer ihr Recht auf Zugang zu den Daten wirksam ausüben können. Die anfallenden Nutzungsdaten müssen auf Anfrage unverzüglich und ggf. kontinuierlich und in Echtzeit zur Verfügung gestellt werden. Gleiches gilt für die Weitergabe von Daten an Dritte. Auch hier ist sicherzustellen, dass Anfragen von Nutzern unverzüglich beantwortet werden können. Hinsichtlich der Weitergabe von Daten an Dritte sind künftig die Modalitäten der Datenübermittlung zwischen dem Dateninhaber und dem Datenempfänger festzulegen. Hierzu ist es notwendig, Vertragsbedingungen für die Bereitstellung von Daten vorzuhalten. Diese Vertragsbedingungen müssen dabei zwingend den Anforderungen 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 ist zu berücksichtigen, dass die Gegenleistung dem Gebot der Angemessenheit entspricht. Um die Angemessenheit der Vergütung beurteilen zu können, müssen sich die Hersteller vernetzter Produkte zunächst über den potenziellen Wert der Daten im Klaren sein. Dies kann eine Heraus-

forderung darstellen, da der Wert von Daten je nach Anwendungskontext stark variieren kann und viele Verwertungsszenarien vage oder unvorhersehbar sind. Bei der Bereitstellung von Daten für Kleinst- und Kleinunternehmen oder gemeinnützige Forschungseinrichtungen ist zudem zu beachten, dass die Gegenleistung nicht höher sein darf als die Kosten, die dem Dateninhaber durch die Bereitstellung der Daten entstehen (Grenzkosten). Bei der Auferlegung von Vertragsbedingungen sind zudem die Vorschriften zur Verhinderung von missbräuchlichen Klauseln im Data Act (Kapitel IV) zu beachten.

Durch die Schaffung von Zugangsrechten besteht die Chance, bisher 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 weiterzugeben, kann zudem die Entwicklung datenbasierter Geschäftsmodelle begünstigen. Gleichzeitig könnten Unternehmen als Reaktion auf die weitreichenden Verpflichtungen des Data Act auch einen Anreiz haben, ihre Produkte so zu gestalten, dass gar keine Nutzungsdaten mehr gespeichert werden oder auf eine Vernetzung der Produkte verzichtet wird. In diesem Fall könnte sich die Menge der potenziell verfügbaren Daten entgegen der Intention des Verordnungsgebers verringern. Aus der Pflicht, Daten für die öffentliche Hand bereitzustellen, können sich Anknüpfungspunkte für Forschungsvorhaben ergeben. Dabei ist jedoch zu beachten, dass der Anwendungsbereich der Bereitstellungspflicht sehr eng gefasst ist. Eine Nutzbarmachung der Daten zu Forschungszwecken kommt nur in außergewöhnlichen Notstandslagen (z. B. Naturkatastrophen, Notlagen im Bereich der öffentlichen Gesundheit) in Betracht und auch nur, wenn der Staat als zugangsberechtigter Akteur die Daten zuvor von den Herstellern angefordert hat. Der tatsächliche Nutzen dieser Datenbereitstellungspflicht für Forschungsvorhaben lässt sich daher derzeit nicht realistisch abschätzen.

3.11 Umsetzungsstand

Nach seiner Verkündung im Amtsblatt der EU ist der Data Act am 11.01.2024 in Kraft getreten. Nach einer Übergangsfrist von 20 Monaten gilt er ab dem 12.09.2025 unmittelbar in der gesamten EU. Die Verpflichtung, vernetzte Produkte und damit verbundene Dienste so zu gestalten, dass die Daten standardmäßig zugänglich sind, gilt abweichend davon erst ein Jahr später ab dem 12.09.2026. Produkte, die bereits vorher in Verkehr gebracht wurden, müssen dieser Verpflichtung nicht nachkommen. Die Regelungen über missbräuchliche Vertragsklauseln gelten für Verträge, die nach dem 12.09.2025 geschlossen werden. Für Verträge, die am oder vor dem 12.09.2025 geschlossen wurden, gelten die Regelungen, wenn diese Verträge unbefristet sind oder ihre Laufzeit frühestens 10 Jahre nach dem 11.01.2024 endet. Die gestaffelten Fristen sollen den Unternehmen und anderen betroffenen Akteuren eine Übergangszeit einräumen, um sich an die neuen Anforderungen der Verordnung anzupassen.

04

4 DIGITAL SERVICES ACT (DSA)

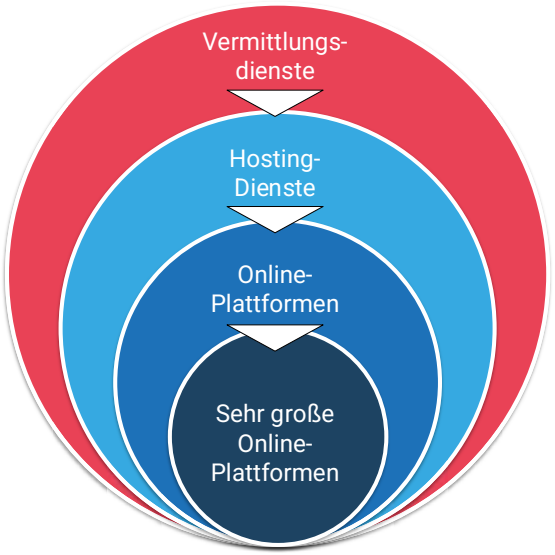
Der Digital Services Act (DSA, Gesetz über digitale Dienste[9]) legt einheitliche Regeln für die Bereitstellung von Vermittlungsdiensten innerhalb der EU fest und ersetzt teilweise die seit 20 Jahren bestehende E-Commerce-Richtlinie. Die Verordnung soll zu einem sicheren, vorhersehbaren und vertrauenswürdigen Online-Umfeld und zum reibungslosen Funktionieren des EU-Binnenmarkts für Vermittlungsdienste beitragen. Zu diesem Zweck 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 festgelegt.

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

4.1 Anwendungsbereich und Adressatenkreis

Der DSA betrifft Anbieter von **Vermittlungsdiensten**, die ihre Dienste gegenüber Nutzern innerhalb der EU anbieten. Dabei spielt es keine Rolle, ob der Anbieter selbst in der EU oder in einem Drittland ansässig ist. Bei den Vermittlungsdiensten wird unterschieden zwischen Anbietern einer „reinen Durchleitung", von „Caching-Leistungen" und von „Hosting-Diensten". Damit wird ein breites Spektrum von Akteuren adressiert. So fallen künftig Online-Marktplätze, Hosting-Anbieter, aber auch Anbieter von Cloud- und Messaging-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)

9 Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste), https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022R2065&from=en.

4.2 Haftungsregeln für Anbieter von Vermittlungsdiensten

Ein zentrales Element des DSA ist die Festlegung von Verantwortlichkeiten für Vermittlungsdienste. Der DSA beschreibt, unter welchen Voraussetzungen diese Dienste von der Haftung für fremde Inhalte befreit sind. Voraussetzung für diese Haftungsprivilegierung ist, dass die Vermittlungsdienste neutral bleiben und die ihnen übermittelten Inhalte lediglich technisch verarbeiten, ohne aktiv darauf Einfluss zu nehmen. Nur wenn der Anbieter trotz Kenntnis rechtswidriger Inhalte nicht handelt, kann er für die Rechtsverletzung verantwortlich gemacht werden. Damit übernimmt der DSA im Wesentlichen die Haftungsprivilegierungen der E-Commerce-Richtlinie. Neu ist die Regelung, dass auch Vermittlungsdienste, die freiwillig Maßnahmen zur Erkennung und Entfernung rechtswidriger Inhalte ergreifen (Good Samaritan Regelung), von der Haftung befreit bleiben. Diese freiwilligen Bemühungen werden honoriert, indem sich auch solche Anbieter auf die Haftungsprivilegierung berufen können.

4.3 Sorgfaltspflichten

Das dritte Kapitel des DSA enthält ein differenziertes Regelwerk zu den Sorgfaltspflichten von Vermittlungsdiensten. Einleitend werden allgemeine Regeln aufgestellt, die für alle Arten von Vermittlungsdienstleistungen gelten. Dazu gehören beispielsweise die Pflicht zur Einrichtung einer zentralen Kontaktstelle oder die Pflicht, in den Allgemeinen Geschäftsbedingungen darzulegen, welche Richtlinien, Verfahren, Maßnahmen und Werkzeuge zur Moderation von Inhalten eingesetzt werden. Hinzu kommen Transparenzpflichten wie die Pflicht zur Veröffentlichung jährlicher Transparenzberichte über Lösch- und Sperraktivitäten. Kleinst- und Kleinunternehmen[10] sind von dieser Pflicht ausgenommen. Eine weitere zentrale Verpflichtung betrifft Hosting-Anbieter. Vorgesehen ist insbesondere die Einrichtung eines Melde- und Abhilfeverfahrens, das es Nutzern ermöglicht, rechtswidrige Inhalte zu melden und entfernen zu lassen.

Zusätzliche Bestimmungen gelten für Online-Plattformen. Online-Plattformen sind Hosting-Diensteanbieter, die Informationen im Auftrag von Nutzern speichern und öffentlich zugänglich machen. Vorgesehen ist beispielsweise die Einrichtung eines internen Beschwerdemanagements für mutmaßlich rechtswidrige Inhalte. Außerdem werden Online-Plattformen verpflichtet, mit zugelassenen außergerichtlichen Streitbeilegungsstellen zusammenzuarbeiten, um Streitigkeiten mit Nutzern ihrer Dienste beizulegen. Eine weitere Regelung betrifft den Umgang mit so genannten „Dark Patterns“. Darunter versteht man die Gestaltung von Benutzeroberflächen, die den Benutzer täuschen, manipulieren oder auf andere Weise in seiner Entscheidungsfindung beeinträchtigen. In diesem Zusammenhang werden u. a. genannt

- die Hervorhebung bestimmter Auswahlkriterien, wenn der Nutzer eine Auswahl treffen soll,
- die wiederholte Aufforderung, eine Auswahl zu treffen, obwohl diese bereits getroffen wurde und
- das Verfahren zur Beendigung eines Dienstes schwieriger zu gestalten als das Verfahren zur Anmeldung.

10 nach Art. 2 der Empfehlung 2003/361/EG sind Kleinstunternehmen Unternehmen mit weniger als 10 Mitarbeitern und einem Jahresumsatz oder einer Jahresbilanzsumme von höchstens 2 Mio. EUR. Kleine Unternehmen sind Unternehmen, die weniger als 50 Mitarbeiter und einen Jahresumsatz oder eine Jahresbilanzsumme von höchstens 10 Mio. EUR haben. Mittlere Unternehmen sind Unternehmen, die weniger als 250 Mitarbeiter und einen Jahresumsatz von höchstens 50 Mio. EUR oder eine Jahresbilanzsumme von höchstens 43 Mio. EUR haben.

Darüber hinaus gelten für Online-Plattformen weitergehende Pflichten, etwa bei der Kennzeichnung von Werbung. So muss unter anderem angegeben werden, in wessen Auftrag die Werbung geschaltet wird, wer für die Werbung bezahlt hat und nach welchen Kriterien die Werbung dem jeweiligen Nutzer angezeigt wird. Transparenzpflichten gelten auch für den Einsatz von Empfehlungssystemen. Anbieter von Online-Plattformen müssen unter anderem darlegen, wie die Empfehlungen zustande kommen und wie die Nutzer auf die Zusammenstellung der Empfehlungen Einfluss nehmen können.

Angebote sehr großer Online-Plattformen mit erheblicher Reichweite (mehr als 45 Millionen Nutzer pro Monat) sind nach Auffassung des Verordnungsgebers mit hohen Risiken verbunden. Diese Anbieter müssen künftig besonders strenge Sorgfaltspflichten erfüllen. Sehr große Plattformen und Suchmaschinen müssen den Missbrauch ihrer Systeme verhindern, indem sie beispielsweise risikobasierte Maßnahmen ergreifen und ihr Risikomanagementsystem unabhängig 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				■
Gewährung des Datenzugangs, damit Behörden Einhaltung der Verordnung prüfen können				■
Mitwirkung an der Ausarbeitung von Verhaltenskodizes				■
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 Datenzugang für Forschende

Der DSA sieht vor, dass sehr große Online-Plattformen autorisierten Forschern Zugang zu bestimmten Datensätzen gewähren müssen. Diese Regelung soll die wissenschaftliche Untersuchung von systemischen Risiken erleichtern, die von diesen Plattformen ausgehen können, wie z. B. die Verbreitung von Desinformation, Auswirkungen auf die öffentliche Sicherheit und die Meinungsfreiheit. Um den Datenschutz zu gewährleisten, müssen die Daten anonymisiert oder pseudonymisiert zur Verfügung gestellt werden. Ziel ist es, Forschende in die Lage zu versetzen, fundierte Analysen und Bewertungen digitaler Plattformen durchzuführen, um deren Einfluss auf die Gesellschaft besser zu verstehen und evidenzbasierte Empfehlungen für politische Maßnahmen zu entwickeln. Der Antrag wird von den Forschenden gestellt. Der Koordinator für digitale Dienste prüft den Antrag auf Qualifikation und Relevanz der Forschungsfrage. Nach erfolgreicher Prüfung wird der Antrag an die jeweilige Online-Plattform weitergeleitet, die verpflichtet ist, die beantragten Daten zur Verfügung zu stellen.

4.5 Durchsetzung und Sanktionen

Die Durchsetzung der Bestimmungen des DSA erfolgt auf zwei Ebenen. Zum einen können Nutzer Schadensersatzansprüche gegen Anbieter gerichtlich geltend machen, wenn diese gegen die Verpflichtungen aus der Verordnung verstoßen. Zum anderen wird die Einhaltung der Verpflichtungen auf nationaler Ebene durch sogenannte „Koordinatoren für digitale Dienste" überwacht. In Deutschland wird diese Aufgabe von der Bundesnetzagentur wahrgenommen. Die Aufsichtsbehörden sind befugt, bei Verstößen Sanktionen zu verhängen. Die Sanktionen müssen wirksam, angemessen und abschreckend sein. Insbesondere sind Bußgelder in Höhe von bis zu sechs Prozent des weltweiten Jahresumsatzes des betroffenen Anbieters im vorangegangenen Geschäftsjahr vorgesehen. Darüber hinaus können bei fortgesetzten Verstößen Zwangsgelder in Höhe von bis zu fünf Prozent des durchschnittlichen weltweiten Tagesumsatzes oder der durchschnittlichen weltweiten Tageseinnahmen des betreffenden Anbieters im vorangegangenen Geschäftsjahr verhängt werden. Daneben sind weitere Instrumente zur Durchsetzung der Vorgaben gegenüber großen Online-Plattformen und Suchmaschinen vorgesehen, über deren Einsatz vorrangig auf EU-Ebene entschieden wird. Hierzu erhält die EU-Kommission entsprechende Ermittlungs- und Durchsetzungsbefugnisse. Als Sanktionsmechanismen sind auch hier die Verhängung von Geldbußen und Zwangsgeldern vorgesehen.

4.6 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 digitale Wirtschaft EU-weit zu vereinheitlichen und national geprägten Regulierungsansätzen entgegenzuwirken. Die Grundsätze zur Verantwortlichkeit von Vermittlungsdiensten für fremde Inhalte haben sich nur geringfügig geändert. Hier gelten im Wesentlichen die aus der E-Commerce-Richtlinie bekannten Haftungsprivilegien weiter. Vermittlungsdienste haften grundsätzlich nicht für Rechtsverletzungen Dritter. Eine Verpflichtung zum Tätigwerden besteht erst ab Kenntnis einer Rechtsverletzung. Das Verfahren zur Meldung und Beseitigung von Rechtsverstößen wird nunmehr verbindlich vorgeschrieben. Darüber hinaus

werden zahlreiche Sorgfaltspflichten eingeführt, deren Umfang mit der Betriebsform des Vermittlungsdienstes und der Anzahl der Nutzer des Dienstes proportional zunimmt. Die größten regulatorischen Belastungen ergeben sich für große Online-Dienste und Suchmaschinen. Darüber hinaus sind auch Auswirkungen auf Forschungs- und Entwicklungsprojekte denkbar. Dies hängt davon ab, ob im Rahmen eines Forschungsprojekts die Vermittlung oder das Hosting fremder Inhalte vorgesehen ist. In diesem Fall sind die Sorgfaltspflichten des DSA anzuwenden. Zu diesem Zweck sollten FuE-Vorhaben entsprechende Aufwände zur Umsetzung der Vorgaben des DSA in ihrer Arbeitsplanung berücksichtigen. In diesem Zusammenhang ist auch zu prüfen, ob ggf. Befreiungen von den Sorgfalts- und Transparenzpflichten zugunsten von Klein- und Kleinstunternehmen einschlägig sind. Die Regelungen des DSA zum Datenzugang für Forschende erleichtern den Zugang zu relevanten Daten von sehr großen Online-Plattformen und ermöglichen Analysen zu systemischen Risiken wie der Verbreitung von Desinformation und den Auswirkungen auf die öffentliche Sicherheit und Meinungsfreiheit. Diese Maßnahmen können evidenzbasierte Empfehlungen für politische Maßnahmen unterstützen. Das Spektrum möglicher Forschungsfragen ist jedoch begrenzt, da der Datenzugang auf die Untersuchung systemischer Risiken beschränkt ist und nicht für andere Forschungsfelder genutzt werden kann.

4.7 Umsetzungsstand

Der DSA wurde am 27.10.2022 im Amtsblatt der Europäischen Union veröffentlicht und gilt seit 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[11] (Digital Markets Act, DMA) sollen einheitliche Wettbewerbsbedingungen auf digitalen Märkten geschaffen werden, auf denen zentrale Plattformdienste mit marktbeherrschender Stellung tätig sind. Darüber hinaus soll der Tendenz entgegengewirkt werden, dass die EU-Mitgliedstaaten nationale Wettbewerbsregeln für Plattformen schaffen, da dies zu einer weiteren Fragmentierung des Binnenmarktes führt.[12]

5.1 Anwendungsbereich und Adressatenkreis

Adressiert werden zentrale Plattformdienste wie Vermittlungsdienste, Suchmaschinen, soziale Netzwerke, App-Stores, Messenger-Dienste oder Anbieter von Video- oder Cloud-Plattformen, sofern sie als sogenannte **Gatekeeper** benannt werden. Die Benennung erfolgt durch die EU-Kommission, wenn bestimmte Kriterien erfüllt sind. Berücksichtigt werden u. a. der Einfluss des Unternehmens auf den Binnenmarkt und das Vorliegen einer dauerhaft gefestigten Marktposition. Die Gate-Keeper-Eigenschaft wird vermutet, wenn bestimmte quantitative Anforderungen erfüllt sind. Dazu gehören der Jahresumsatz (7,5 Milliarden Euro) und die Anzahl der aktiven Nutzer (45 Millionen). Unternehmen haben die Möglichkeit, gegen die Benennung vorzugehen. Dazu müssen sie nachweisen, dass die Voraussetzungen der Gate-Keeper-Eigenschaft trotz Überschreitens der Schwellenwerte nicht vorliegen. Bei Erreichen der Schwellenwerte müssen Unternehmen, die zentrale Plattformdienste erbringen, dies der EU-Kommission unverzüglich anzeigen.

5.2 Verhaltenspflichten für Gatekeeper

Gatekeeper müssen nach dem DMA eine Reihe von Ge- und Verboten beachten. So ist es beispielsweise untersagt, personenbezogene Daten innerhalb eines Konzerns zusammenzuführen. Eine solche Zusammenführung von Datenbeständen ist nur noch mit ausdrücklicher Einwilligung des Betroffenen 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. Darüber hinaus gibt es eine Reihe von Verbotstatbeständen, die im Wesentlichen darauf abzielen, wettbewerbswidrige Praktiken großer Plattformen zu unterbinden. So ist es beispielsweise untersagt, eigene Produkte oder Dienste besser zu behandeln als Dienste Dritter oder Daten von gewerblichen Nutzern, mit denen der Gatekeeper im Wettbewerb steht, für eigene Zwecke zu verwenden.

5.3 Durchsetzung und Sanktionen

Die EU-Kommission ist für die Durchsetzung der Vorgaben des DMA zuständig. Verstößt ein Gatekeeper gegen eine ihm obliegende Verpflichtung, kann die EU-Kommission eine Untersuchung wegen Nichteinhaltung einleiten. Im Rahmen des Nichteinhaltungsbeschlusses können Geldbußen in Höhe von bis zu zehn Prozent des letzten Jahresumsatzes verhängt werden. Dabei werden die Schwere, die Dauer und eine etwaige Wiederholung des Verstoßes berücksichtigt. Voraussetzung ist, dass der Gatekeeper seine Pflichten vorsätzlich oder fahrlässig verletzt hat. Neben dem

11 Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte), https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022R1925.

12 Vgl. Erwägungsgrund 6 des DMA.

behördlichen Sanktionsregime besteht auch die Möglichkeit, Verstöße privatrechtlich zu verfolgen. Das bedeutet, dass auch (gewerbliche und private) Nutzer oder Wettbewerber die Einhaltung der Verordnung einklagen und – bei Vorliegen der Voraussetzungen – 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. Das Regulierungsvorhaben zielt vor allem darauf ab, den Aktionsradius marktmächtiger Plattformkonzerne einzuschränken und wettbewerbsbeschränkende Geschäftspraktiken zu unterbinden. Damit besteht die Chance, die Rahmenbedingungen für den Wettbewerb zu verbessern, unter denen FuE-Projekte, aber auch kleine und mittlere Unternehmen agieren. Ob die Verordnung tatsächlich zu offeneren und faireren Märkten führt, kann derzeit noch nicht abschließend beurteilt werden. Entscheidend wird sein, inwieweit die im DMA vorgesehenen Kontroll- und Sanktionsmechanismen tatsächlich angewandt werden.

5.5 Umsetzungsstand

Der DMA 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 weitere nationale Umsetzungsakte seit dem 02.05.2023 in der gesamten EU. Ab diesem Zeitpunkt sind Unternehmen, die zentrale Plattformdienste anbieten, verpflichtet, der EU-Kommission ihren möglichen Status als Gatekeeper mitzuteilen. Die EU-Kommission hat die ersten Benennungsbeschlüsse im September 2023 erlassen. Die als Gatekeeper benannten Unternehmen haben ab diesem Zeitpunkt sechs Monate Zeit, um ihren Verpflichtungen nachzukommen.

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 (2020): 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 (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.

ANHANG

ANHANG

Glossar

BEGRIFF	ERLÄUTERUNG
Artificial Intelligence Act – AI Act	Siehe KI-Verordnung
Data Governance Act (DGA)	Der DGA schafft einen Rechtsrahmen, der die Verfügbarkeit, den Zugang und die gemeinsame Nutzung von Daten innerhalb der EU erleichtern soll.
Datenempfänger	Ein Datenempfänger im Sinne des Data Act ist eine Person oder Organisation, die in Ausübung ihrer beruflichen Tätigkeit handelt und kein Nutzer vernetzter Produkte oder Dienste ist und der vom Dateninhaber Daten zur Verfügung gestellt werden, einschließlich Dritter, denen der Dateninhaber auf Verlangen des Nutzers oder aufgrund gesetzlicher Vorschriften Daten zur Verfügung stellt.
Dateninhaber	Ein Dateninhaber ist eine Person oder Organisation, die nach dem Data Act, nach geltendem Unionsrecht oder nationalen Vorschriften berechtigt oder verpflichtet ist, Daten zu nutzen und bereitzustellen, einschließlich Produkt- und Dienstdaten, die während der Erbringung eines verbundenen Dienstes abgerufen oder generiert wurden.
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 Geschäftsbeziehungen zwischen 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 auf EU-Ebene ist ein rechtliches Instrument, das von der Europäischen Kommission erlassen wird, um die einheitliche Anwendung und Umsetzung von EU-Rechtsvorschriften in den Mitgliedstaaten sicherzustellen. Diese Rechtsakte konkretisieren die allgemeinen Regeln und Prinzipien, die in EU-Verordnungen und -Richtlinien festgelegt sind, und geben detaillierte Anweisungen zur praktischen Durchführung dieser Vorschriften. Durchführungsrechtsakte werden häufig genutzt, um technische Details, Verfahren oder Standards festzulegen, die für die effiziente und einheitliche Anwendung der EU-Gesetze erforderlich sind. Sie werden gemäß einem festgelegten Verfahren erlassen, das die Beteiligung von Experten aus den Mitgliedstaaten und gegebenenfalls des Europäischen Parlaments und des Rates vorsieht.

BEGRIFF	ERLÄUTERUNG
Europäische Datenstrategie	Mit der Europäischen Datenstrategie hat sich die Europäische Kommission zum Ziel gesetzt, einen europäischen Binnenmarkt für Daten zu etablieren. Die Datenweitergabe zwischen Unternehmen, Forschenden und öffentlichen Verwaltungen soll so verbessert werden.
FRAND-Bedingungen	FRAND-Bedingungen (FRAND = Fair, Reasonable and Non Discriminatory terms) bedeuten, dass Lizenzen (insbesondere für Patente) auf faire, angemessene und nichtdiskriminierende Weise vergeben werden müssen.
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 anderer 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 Betreiber von KI-Systemen müssen die Vorgaben der KI-Verordnung künftig umsetzen.

Die Verordnung ist anwendbar auf KI-Systeme, also auf maschinenbasierte Systeme, die selbstständig arbeiten, sich anpassen und aus Daten Schlussfolgerungen ziehen können, um Vorhersagen, Empfehlungen oder Entscheidungen zu treffen.

Die KI-Verordnung schließt KI-Systeme unter freier oder offener Lizenz sowie solche, die ausschließlich für wissenschaftliche Forschung und Entwicklung entwickelt wurden, aus ihrem Anwendungsbereich aus, sofern diese Systeme nicht verboten oder als hochriskant eingestuft sind.

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.

Die 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 Definition von KI-Systemen könnte zu Interpretationsschwierigkeiten bei der Frage führen, ob die entwickelte Software oder das Produkt als KI-System anzusehen ist.

KI-Systeme unter freier/offener Lizenz und solche für reine Forschung und Entwicklung, sofern nicht verboten oder hochriskant, sind vom Anwendungsbereich ausgenommen, was eine Erleichterung bei Forschungs- und Entwicklungstätigkeiten bedeuten kann.

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/Betreiber der KI für die Umsetzung der Anforderungen der KI-Verordnung verantwortlich ist.

Von KI-Reallaboren können positive Impulse für das Innovationsgeschehen ausgehen. Die Rahmenbedingungen sind jedoch eher restriktiv ausgestaltet und bedingen einen hohen Abstimmungsbedarf mit den Aufsichtsbehörden.

AKTUELLER UMSETZUNGSSTAND

Die KI-Verordnung ist am 01.08.2024 in Kraft getreten und gilt unmittelbar ab dem 02.08.2026.

Die Vorschriften für verbotene KI-Systeme gelten abweichend hiervon bereits ab dem 02.02.2025.

Die Verpflichtungen für Hochrisiko-KI-Systeme müssen ab dem 02.08.2027 eingehalten werden.

Gewisser Bestandsschutz besteht für KI-Systeme, die vor 2026 entwickelt und in Betrieb genommen werden.

DATA GOVERNANCE ACT

WORUM GEHT ES?

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

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

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

Datenvermittlungsdienste müssen von einer gesonderten juristischen Person erbracht werden. Eine behördliche Registrierung und die Einhaltung zahlreicher Anforderungen sind erforderlich.

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

Verstöße gegen die Verordnung können behördlich sanktioniert werden.

ZENTRALE AUSWIRKUNGEN

Die Verfügbarkeit von öffentlich zugänglichen Daten (Open Data) könnte perspektivisch verbessert werden.

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

Datenvermittlungsdienste dürfen Daten nicht monetarisieren. Es muss eine strikte Trennung zwischen Datenvermittlung und Datennutzung bestehen. Der Datenvermittlungsdienst muss von einer separaten juristischen Person angeboten werden. FuE-Projekte müssen die Bereiche Datenvermittlung/Angebot von datenbasierten Diensten trennen. Beispielsweise ist ein Forschungspartner für die Datenvermittlungsplattform zuständig, der andere für das Angebot von KI-Diensten. Bei der Entwicklung des Geschäftsmodells ist zu berücksichtigen, dass das Angebot eines reinen Vermittlungsdienstes finanziell nicht tragfähig sein kann.

Datenaltruistische Organisationen könnten die Erschließung neuer Datenbestände fördern.

AKTUELLER UMSETZUNGSSTAND

Der DGA wurde am 03.06.2022 verabschiedet und ist seit 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 standardmäßig zugänglich gestalten (Accessibility by Default/Design) und die Nutzer über die Möglichkeiten des Datenzugriffs informieren.

Die Nutzer haben ein Recht auf Zugang zu den von ihnen erzeugten Daten. Darüber hinaus kann die Bereitstellung von Daten an Dritte verlangt werden.

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

Der Data Act enthält eine Reihe von Bestimmungen zugunsten von KMU, die diese vom Anwendungsbereich der Verordnung ausnehmen oder sie vor unfairen Wettbewerbshandlungen schützen sollen.

In Notstandslagen können auch öffentliche Stellen Zugang zu Daten verlangen.

Der Wechsel zwischen Cloud-Anbietern wird 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 Nutzer diesen und/oder Dritten Daten zugänglich machen (in Notstandslagen auch öffentlichen Stellen). Dies bietet Potenzial für neue Anwendungsfelder und datenbasierte Geschäftsmodelle.

In FuE-Projekten bedarf es einer Abstimmung zwischen den Akteuren, wie die Vorgaben des Data Act umgesetzt werden.

Die Pflicht zur Datenbereitstellung für öffentliche Stellen und mit ihnen verbundene Forschungseinrichtungen ist für die Forschung von begrenztem Nutzen, da die Bereitstellungspflicht auf Notfallsituationen beschränkt ist.

Hersteller müssen die vertraglichen Bedingungen der Datenbereitstellung rechtskonform gestalten. Dies setzt u. a. voraus, dass eine mögliche Vergütung festgelegt wird. Das Datenvertragsrecht gewinnt in diesem Zusammenhang erheblich an Bedeutung. Kleinere Unternehmen und gemeinnützige Forschungseinrichtungen können profitieren, da für sie die Vergütung nicht höher sein darf als die Grenzkosten der Datenbereitstellung.

AKTUELLER UMSETZUNGSSTAND

Der Data Act gilt EU-weit ab dem 12.09.2025.

Die Verpflichtung, vernetzte Produkte und Dienstleistungen so zu gestalten, dass sie standardmäßig Daten bereitstellen können, gilt jedoch erst ab dem 12.09.2026; vorher in Verkehr gebrachte Produkte sind davon ausgenommen.

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 monatlich Nutzende) 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 Nutzer 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 seit 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. Gatekeeper (Torwächter) benannt wurden.

Die Gatekeeper-Eigenschaft bemisst sich u. a. nach der Anzahl der aktiven Nutzer (45 Millionen) und dem Jahresumsatz (7,5 Milliarden Euro).

Es werden zahlreiche Ge- und Verbote für Gatekeeper aufgestellt, etwa im Zusammenhang mit Werbung, Transparenz und in Bezug auf wettbewerbswidrige 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 sind überschaubar. Dennoch verbessern sich durch den Rechtsakt die allgemeinen wettbewerblichen Rahmenbedingungen.

AKTUELLER UMSETZUNGSSTAND

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