GDD-Praxishilfe

Europäische Datenstrategie: KI-VO, Data Act etc.

- Adressaten und Regelungsschwerpunkte der neuen Digitalakte -

INHALT

EINLEITUNG

Die Europäische Union (EU) sieht sich mit der Herausforderung konfrontiert, den digitalen Wandel zu gestalten, ohne grundlegende Werte des Datenschutzes und der Datensicherheit zu vernachlässigen. Angesichts der rasanten technologischen Entwicklungen und der zunehmenden Digitalisierung aller Lebensbereiche ist es von entscheidender Bedeutung, einen ausgewogenen rechtlichen Rahmen zu schaffen, der sowohl Innovationen fördert als auch die Privatsphäre der Bürgerinnen und Bürger schützt.

Mit der Europäischen Datenstrategie verfolgt die EU das Ziel, sich an die Spitze einer datengesteuerten Gesellschaft zu bringen. Durch einen Daten-Binnenmarkt soll eine EU-weite und branchen-übergreifende Datenweitergabe zum Nutzen von Unternehmen, Forschenden und öffentlichen Verwaltungen ermöglicht werden, wodurch Innovationen gefördert und das Wachstum angeregt werden sollen. Durch die Gewährung eines verbesserten Zugangs zu Daten wird es Unternehmen erleichtert, hochwertigere und nachhaltigere Produkte sowie Dienste herzustellen und anzubieten, was schließlich auch den Verbrauchern zugutekommt. Der deutsche Gesetzgeber sieht das und hat die neuen Datenakte und deren Verhältnis zur DS-GVO vor dem Digitalausschuss des Deutschen Bundestages im Juni 2024 diskutiert und Handlungsoptionen für eine datenschutzkonforme Datenteilung mit Sachverständigen unter Überschrift: Innovative Datenpolitik: Potenziale und Herausforderungen erörtertet.[1] Das Datenschutzrecht – so wurde konstatiert - entwickelt sich mit Geltung der neuen Datenakte zunehmend auch zu einem Datenwirtschaftsrecht. Grundlage hierfür ist schon Art. 1 DS-GVO, der zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten verpflichtet.[2]

Diese Praxishilfe ordnet die neue Entwicklung ein. Es werden die wichtigsten Rechtsakte, die im Rahmen der Europäischen Datenstrategie geplant oder bereits verabschiedet worden sind, überblickartig dargestellt und in ihren datenschutzrechtlichen Auswirkungen eingeordnet. Besonderes Augenmerk gilt hierbei auch Stellung und Aufgaben des Datenschutzbeauftragten, der sich in Bezug auf die in Rede stehenden Rechtsakte mit neuen Aufgaben konfrontiert sieht.

1 Abrufbar unter: https://www.bundestag.de/ausschuesse/a23_digitales/Anhoerungen/1006274-1006274.
2 Schwartmann, Stellungnahme vor dem Digitalausschuss des Deutschen Bundestages vom 26.06.2024: https://www.bundestag.de/resource/blob/1010058/15b3c22909f8abd112260e5eaa1cfdc1/Stellungnahme-Schwartmann.pdf

A. Die Europäische Datenstrategie im Überblick

I. Allgemeines

Die Europäische Datenstrategie der EU ist ein Projekt zur Regulierung der digitalen Wirtschaft. Angestrebt wird die Schaffung eines sicheren, auf den Menschen ausgerichteten digitalen Ökosystems, in dem die Bürgerinnen und Bürger gestärkt werden und die Unternehmen vom digitalen Potenzial profitieren.

Diese GDD-Praxishilfe bietet einen Überblick über die im Rahmen der EU-Datenstrategie neugeschaffenen bzw. geplanten Rechtsakte, die sich wie folgt kategorisieren lassen:

II. Daten- und Cyberstrategie

Der bereits geltende **Data Governance Act (DGA)** bildet gemeinsam mit dem Data Act eine zentrale Säule der EU-Datenstrategie. Gemeinsames Ziel ist die Förderung der Wertschöpfung aus Daten durch entsprechende rechtliche Rahmenbedingungen. Der DGA richtet sich primär an öffentliche Stellen, Datenvermittlungsdienste und datenaltruistische Organisationen und soll mehr Daten verfügbar machen sowie den Datenaustausch zwischen Sektoren und EU-Ländern erleichtern, um das Potenzial der Daten zum Nutzen der europäischen Bürger und Unternehmen zu nutzen. Hierdurch sollen datengesteuerte Innovationen in den Bereichen Gesundheit, Mobilität, Umwelt, Landwirtschaft und öffentliche Verwaltung ermöglicht werden. Der DGA erfasst personenbezogene wie nicht personenbezogene Informationen. Soweit personenbezogene Daten betroffen sind, sind zudem die Vorgaben der DS-GVO zu beachten.

Zentrales Element des **Data Act (DA)** ist die Pflicht, **Daten, die bei der Nutzung von vernetzten Produkten**, z.B. Haushaltsgeräten oder Autos, oder **sog. verbundenen Diensten entstehen, für den Nutzer zugänglich zu machen**, idealerweise durch direkten Zugriff. So soll der DA etwa Nutzern ermöglichen, problemlos zwischen Cloud-Anbietern zu wechseln. Der DA betrifft Daten, die bei der Nutzung von vernetzten Produkten oder verbundenen Diensten erzeugt werden, unabhängig von einem Personenbezug. Der Anwendungsbereich des DA ist insofern weiter als derjenige der DS-GVO. Der DA hat für Unternehmen nicht nur Relevanz, weil sie als potenzielle Adressaten ggf. die aus diesem resultierenden Pflichten einhalten müssen, sondern auch als potenziell anspruchsberechtigte Nutzer, sofern vernetzte Produkte oder verbundene Dienste verwendet werden. Der DA ist am 11. Januar 2024 in Kraft getreten und gilt **ab dem 12. September 2025 als EU-weit direkt anwendbares Recht**. Für Details zu den Regelungen des DA vgl. im Einzelnen Abschnitt C in dieser Praxishilfe.

Der **Cyber Resilience Act (CRA) (Entwurf)** zielt darauf ab, Verbraucher und Unternehmen zu schützen, die **Produkte mit einer digitalen Komponente** kaufen oder verwenden. Produkte mit digitalen Elementen sollen nur auf den Markt gebracht werden dürfen, wenn sie bestimmte wesentliche Anforderungen an die Cybersicherheit erfüllen. Der CRA soll gelten für alle Produkte, die direkt oder indirekt mit einem anderen Gerät oder Netzwerk verbunden sind, mit Ausnahme bestimmter Ausnahmen wie Open-Source-Software oder Dienste, die bereits durch bestehende Vorschriften abgedeckt sind. Mit Inkrafttreten der Verordnung sollen mit dem Internet verbundene Software und Produkte die CE-Kennzeichnung tragen, um anzuzeigen, dass sie den neuen Normen entsprechen. Vorgesehen sind **Verpflichtungen für Hersteller, Händler und Importeure** entsprechender Produkte bzw. Software.

Die **NIS-2-Richtlinie** ist eine EU-weite Gesetzgebung zur **Cybersicherheit** und enthält Vorgaben zur Steigerung des Niveaus der Cybersicherheit in der EU. Die Richtlinie adressiert **nicht alle Unternehmen und Organisationen,**

sondern nur solche aus besonders relevanten näher definierten Sektoren. Im Vergleich zur ersten NIS-Richtlinie aus dem Jahr 2016 wird durch die NIS-2-Richtlinie allerdings der Kreis der Verpflichteten deutlich erweitert. Die Einrichtungskategorie KRITIS als Kategorie für Unternehmen, die besonders schützenswert sind, wird fortgeführt. Neu eingeführt werden daneben die Einrichtungskategorien „besonders wichtige Einrichtungen" und „wichtige Einrichtungen".[3] Darüber hinaus werden höhere Anforderungen an die Informationssicherheit der betroffenen Organisationen gestellt sowie Meldepflichten erweitert. EU-Richtlinien sind anders als EU-Verordnungen in den Mitgliedstaaten nicht unmittelbar verbindlich, vielmehr bedarf es der **Umsetzung in nationales Recht**. Die Frist zur Umsetzung der Richtlinie durch die Mitgliedstaaten läuft bis zum 17. Oktober 2024. Auf deutscher Ebene existiert aktuell erst ein Referentenentwurf des zuständigen Bundesinnenministeriums für ein „NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz" (Stand: 07.05.2024).[4]

III. Digitale Plattformen und Dienstleistungen

Über den **Digital Services Act (DSA)** sollen ein sichereres und verantwortungsvolles Online-Umfeld geschaffen, die Verbreitung von Desinformationen verhindert sowie Nutzer und Nutzerinnen besser geschützt werden. Die Verpflichtungen des DSA richten sich an **Online-Vermittler und Online-Plattformen** wie z.B. Online-Marktplätze, Reiseportale oder soziale Netzwerke, soweit die Vermittler bzw. Plattformen ihre Dienste in der EU anbieten. Für sehr große Online-Plattformen und sehr große Suchmaschinen sind aufgrund der mit diesen einhergehenden besonderen Risiken spezielle Regelungen vorgesehen. **Seit dem 17. Februar 2024 gilt der DSA vollumfassend und unmittelbar in den EU-Mitgliedstaaten**. In Deutschland wird der DSA durch das **„Digitale-Dienste-Gesetz (DDG)"** ergänzt, welches am 14. Mai 2024 in Kraft getreten ist. Das DDG schafft vor allem einen Rahmen für die behördliche Überwachung der Bestimmungen des DSA in Deutschland (zu den Zuständigkeitsregelungen vgl. im Einzelnen Abschnitt C in dieser Praxishilfe).

Mit dem **Digital Markets Act (DMA)** wurden besondere Vorgaben für sog. **Gatekeeper-Plattformen** eingeführt, um die Märkte im digitalen Sektor gerechter, offener und fairer zu machen. Der DMA stellt Verhaltensregelungen für die großen Digitalunternehmen auf und beschränkt die Macht marktbeherrschender Unternehmen, z.B. durch Selbstbegünstigungsverbote, Regelungen zur Datennutzung und zur Dateninteroperabilität und Diskriminierungsverbote.

IV. Rechtlicher Rahmen für KI

Als weltweit erstes umfassendes Regelungswerk für diesen Bereich setzt die KI-VO den **rechtlichen Rahmen für den Einsatz von Künstlicher Intelligenz (KI)** in Europa. Zielsetzung ist hierbei einerseits Innovationen zu fördern und das Vertrauen in KI zu stärken und andererseits, sicherzustellen, dass KI nur in einer Weise genutzt wird, welche die Grundrechte und die Sicherheit der Bürgerinnen und Bürger der EU respektiert. Verfolgt wird dabei ein **risikobasierter Ansatz**: Je höher das Risiko, welches von einem KI-System ausgeht, desto weitergehend sind die Pflichten. So sind bei Anwendungen mit geringem Risiko lediglich bestimmte Transparenz- und Informationspflichten einzuhalten. Anwendungen mit inakzeptablem Risiko sind demgegenüber verboten. Hierzu zählen z.B. Anwendungen im Bereich des Social Scoring, sofern es zu einer Schlechterstellung

3 Die betroffenen Sektoren sind im Gesetzentwurf in Form von Anlagen gelistet (vgl. den in der nächsten Fußnote verlinkten Gesetzesentwurf, S. 70 ff.).
4 https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwuerfe/CI1/NIS-2-RefE.pdf?__blob=publicationFile&v=5.

oder Benachteiligung kommt. Social Scoring meint die Klassifizierung von Menschen auf der Grundlage ihres Sozialverhaltens, ihres sozioökonomischen Status oder persönlicher Merkmale. Die KI-VO, die **unmittelbare Geltung in Deutschland** entfaltet, richtet sich an eine **Reihe verschiedener Adressaten**. Hauptadressat ist der „Anbieter", der das KI-System bzw. -Modell entwickelt hat. Pflichten nach der VO treffen aber auch **„Betreiber"** entsprechender Systeme, also insbes. Unternehmen, welche KI-Systeme einsetzen. Details zu den Regelungen der KI-VO vgl. die Detailausführungen im nachfolgenden Abschnitt B.

Die KI-VO soll ergänzt werden um eine **EU-Richtlinie über die Haftung für KI**, mit der neue Vorschriften speziell für durch KI-Systeme verursachte Schäden eingeführt werden sollen. Hintergrund der geplanten Richtlinie ist, dass die aktuell geltenden nationalen Haftungsvorschriften für Schadenersatzansprüche infolge von Schäden durch KI nicht ausgelegt sind. Eingeführt werden sollen insbes. Erleichterungen der Beweislast zugunsten der Geschädigten, auch soll der Zugang Geschädigter zu einschlägigen Beweismitteln erleichtert werden.[5] Geschützt werden sollen nicht nur geschädigte natürliche Personen, sondern auch Unternehmen und sonstige Organisationen, welche einen Schaden aufgrund KI erlitten haben.[6] Die Richtlinie befindet sich aktuell noch im Gesetzgebungsverfahren. Anders als die KI-VO wird die geplante Richtlinie **keine unmittelbare Wirkung** in den Mitgliedstaaten entfalten, sondern muss von diesen zunächst innerhalb einer Umsetzungsfrist in nationales Recht umgesetzt werden.

5 Vgl. auch EU-Kommission, Fragen und Antworten: Richtlinie über KI-Haftung v. 28.09.2022, abrufbar über nachfolgenden Link: https://ec.europa.eu/commission/presscorner/detail/de/qanda_22_5793.
6 Vgl. EU-Kommission, Fragen und Antworten: Richtlinie über KI-Haftung v. 28.09.2022, vgl. vorstehende Fußnote.

B. KI-Verordnung (KI-VO)

I. Inkrafttreten und Geltung

Das Gesetz über Künstliche Intelligenz (KI-VO) tritt am 1. August 2024 in Kraft. **Anwendung in den Mitgliedstaaten findet sie dann grundsätzlich nach 24 Monaten**. Einige Vorschriften sind allerdings schon vorher zu beachten: So müssen Maßnahmen zur Vermittlung von KI-Kompetenz, die sich grundsätzlich an jedermann richten, nach sechs Monaten ergriffen sein und die Vorschriften zu den KI-Modellen mit allgemeinem Verwendungszweck bereits nach 12 Monaten. Komplett anwendbar ist die KI-VO 36 Monate nach Inkraftreten.[7]

II. Grundsätzliches: Risikobasierter Ansatz

Wie bereits erwähnt, folgt die KI-VO einem risikoorientierten Ansatz.[8] Vereinfacht bedeutet dies: Je höher das Risiko des KI-Systems[9], desto strenger die Pflichten, welche die Adressaten der KI-VO zu beachten haben. **KI-Systeme mit inakzeptablem Risiko** sind verboten (vgl. Art. 5 KI-VO **„Verbotene Praktiken im KI-Bereich"**).[10]

KI-Systeme mit hohem Risiko sind solche, welche sich potenziell nachteilig auf die Sicherheit der Menschen oder ihre Grundrechte auswirken. Die KI-Verordnung sieht **zwei Arten** von Hockrisiko-KI-Systemen vor (vgl. im Einzelnen Art. 6 KI-VO).[11]

Zum einen werden KI-Systeme, die **Sicherheitskomponenten von Produkten oder selbst Produkte** sind, die in den Anwendungsbereich

7 Ein Zeitplan findet sich bei Schwartmann/Kurth in Schwartmann/Keber/Zenner (Hrsg.), Leitfaden KI-VO (nachfolgend LF KI-VO), 1. Teil 1. Kap. Rn. 1 ff.
8 Dazu Schwartmann/Köhler in LF KI-VO, 2. Teil 1. Kap. Rn. 51 ff.
9 Dieser Zentralbegriff ist in Art. 3 Nr. 1 KI-VO definiert. Dazu LF KI-VO, 2. Teil 1. Kap. Rn. 12 f.
10 Zu Art. 5 KI-VO vgl. auch Abschnitt IV.
11 Dazu grundlegend Schwartmann/Köhler in LF KI-VO, 2. Teil 1. Kap. Rn. 125 ff.

bestimmter **Harmonisierungsrechtsvorschriften der Union** fallen, als hochriskant eingestuft, wenn das Produkt gemäß den Vorschriften einem Konformitätsbewertungsverfahren durch Dritte unterzogen wird. Beispiele sind etwa Kraftfahrzeuge, Spielzeuge, Medizinprodukte.

Zum anderen sind in **Annex III der KI-VO** bestimmte Anwendungsbereiche aufgezählt, die zur Einordnung als Hochrisiko-KI-System führen.[12] Hierzu gehören etwa näher beschriebene Anwendungen in den Bereichen biometrische Identifizierung, kritische Infrastrukturen, Beschäftigung und Personalmanagement, Strafverfolgung, Migration und Grenzkontrolle. Die Liste kann überarbeitet werden, um sie an die Entwicklung anzupassen. Bzgl. der Einstufung der im Annex III genannten KI-Systeme als Hochrisiko-Systeme sieht allerdings Art. 6 Abs. 3 KI-VO eine Gegenausnahme vor. Trotz Nennung im Anhang III gilt ein KI-System nicht als hochriskant, wenn es kein erhebliches Risiko der Beeinträchtigung in Bezug auf die Gesundheit, Sicherheit oder Grundrechte natürlicher Personen birgt, indem es unter anderem nicht das Ergebnis der Entscheidungsfindung wesentlich beeinflusst. Für das Eingreifen der Gegenausnahme und damit das Nichtvorliegen eines Hochrisikosystems spricht es, wenn eine der nachfolgenden Bedingungen erfüllt ist:

>> Zweck des Systems ist (nur) eine eng gefasste prozessuale Aufgabe zu erledigen.
>> Zweck des Systems ist (nur), das Ergebnis einer davor abgeschlossenen menschlichen Entscheidung zu verbessern.
>> Das System soll nur Entscheidungsmuster oder Abweichungen erkennen, ohne eine zuvor durchgeführte menschliche Beurteilung zu ersetzen oder zu beeinflussen.
>> Es erfolgen nur vorbereitende Aufgaben für eine in Annex III genannte Bewertung.[13]

Zu den **Pflichten im Zusammenhang mit Hochrisikosystemen** vgl. unter IV.[14]

KI-Systeme, die nicht im vorbeschriebenen Sinne als hochriskant anzusehen sind, **die** aber **mit natürlichen Personen interagieren oder Inhalte erzeugen** sollen, haben insbes. die Transparenzvorgaben nach Art. 50 KI-VO zu beachten. Danach sollen natürliche Personen insbes. mitgeteilt bekommen, wenn sie es mit einem KI-System zu tun haben. KI-Systeme, die mit Personen interagieren, sind **etwa Chatbots**.

KI-Systeme, die weder hochriskant sind noch in den Anwendungsbereich von Art. 50 DS-GVO fallen, unterliegen keinen speziellen Vorgaben nach der KI-VO. Solche Systeme dürfen unter Einhaltung der allgemein geltenden Regeln entwickelt und verwendet werden. Zu diesen allgemeinen Regelungen zählt auch die DS-GVO, sofern bei der Entwicklung des Systems bzw. bei dessen Einsatz personenbezogene Daten verarbeitet werden.

III. Adressaten der KI-VO

Adressaten der KI-VO sind nach dessen Art. 2 Abs. 1

>> **Anbieter**, die in der Union KI-Systeme in Verkehr bringen oder in Betrieb nehmen oder KI-Modelle mit allgemeinem Verwendungszweck in Verkehr bringen, unabhängig davon, ob diese Anbieter in der Union oder in einem Drittland niedergelassen sind;
>> **Betreiber** von KI-Systemen, die ihren Sitz in der Union haben oder sich in der Union befinden;

12 Zu den Anwendungsbereichen im Einzelnen Hansen/Nägele/Steinbrück in LF KI-VO, 2. Teil 1. Kap. Rn. 165 ff.
13 Dazu ausführlich Schwartmann/Köhler in LF KI-VO, 2. Teil 1. Kap. Rn. 129 ff.
14 Dazu auch Kremer/Haar in LF KI-VO, 2. Teil 1. Kap. Rn. 364 ff.

>> **Anbieter und Betreiber** von KI-Systemen, die ihren Sitz in einem Drittland haben oder sich in einem Drittland befinden, wenn das vom System hervorgebrachte Ergebnis in der Union verwendet wird;
>> **Einführer und Händler** von KI-Systemen;
>> **Produkthersteller**, die KI-Systeme zusammen mit ihrem Produkt unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringen oder in Betrieb nehmen;
>> Bevollmächtigte von Anbietern, die nicht in der Union niedergelassen sind;
>> betroffene Personen, die sich in der Union befinden.

Die zugehörigen **Begriffsbestimmungen** enthält Art. 3 KI-VO.

Anbieter im Sinne der KI-VO ist demnach „eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System oder ein KI-Modell mit allgemeinem Verwendungszweck entwickelt oder entwickeln lässt und es unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringt oder das KI-System unter ihrem eigenen Namen oder ihrer Handelsmarke in Betrieb nimmt, sei es entgeltlich oder unentgeltlich".

Betreiber im Sinne der KI-VO ist „eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System in eigener Verantwortung verwendet, es sei denn, das KI-System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet".

Unternehmen, welche KI einsetzen, können als Betreiber, aber auch als Anbieter Adressaten der KI-VO sein. Beispiele: Ein Unternehmen, das einen eigenen KI-Chatbot entwickelt bzw. entwickeln lässt und diesen auf der Unternehmenswebsite einsetzt, ist „Anbieter" i.S.d. KI-VO. Ein Unternehmen, dass Microsoft Copilot einsetzt, ist „Betreiber" i.S.d. KI-VO.

IV. Zentrale Regelungen der KI-VO, insbes. Pflichten von Anbietern und Betreibern

Im **Kapitel I** der KI-VO kommt neben Vorschriften zum Zweck und Anwendungsbereich der Verordnung (Artt. 1 und 2) sowie den Begriffsbestimmungen (Art. 3) praktische Relevanz insbes. auch der mit „KI-Kompetenz" überschriebenen Bestimmung in Art. 4 zu. Nach der genannten Bestimmung haben Anbieter und Betreiber von KI-Systemen Maßnahmen zu ergreifen, um nach besten Kräften sicherzustellen, dass ihr Personal und andere Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, über ein ausreichendes Maß an KI-Kompetenz verfügen, wobei ihre technischen Kenntnisse, ihre Erfahrung, ihre Ausbildung und Schulung und der Kontext, in dem die KI-Systeme eingesetzt werden sollen, sowie die Personen oder Personengruppen, bei denen die KI-Systeme eingesetzt werden sollen, zu berücksichtigen sind.

Sofern Unternehmen KI verwenden, müssen hierzu eingesetzte Beschäftigte in ausreichendem Maß geschult sein („KI-Kompetenz").

Im **Kapitel II** enthält die KI-VO einen **Katalog mit verbotenen Praktiken (Art. 5)**. Im Einzelnen werden folgende Praktiken im Zusammenhang mit KI als unvereinbar mit den Grundrechten der EU angesehen und sind daher grundsätzlich[15] verboten:[16]

>> **Unterschwellige Verhaltensbeeinflussung**
>> Beeinflussung und **Ausnutzung schutzbedürftiger Gruppen**

15 Teilweise sehen die einzelnen Tatbestände Ausnahmen von den Verboten vor (zum konkreten Verbotsinhalt vgl. jeweils den Gesetzeswortlaut).
16 Schwartmann/Pottkämper in LF KI-VO, 2. Teil 1. Kap. Rn. 57 ff.

>> **Social Scoring** und Verhaltensvorhersagen, sofern hiermit eine Benachteiligung verbunden ist
>> **Risikobewertung** mit Blick auf **kriminelles Verhalten**
>> Erstellung von **Datenbanken zur Gesichtserkennung** durch ungezieltes Auslesen von Gesichtsbildern aus dem Internet bzw. Erweiterung solcher Datenbanken
>> **Ableitung von Emotionen am Arbeitsplatz und in Bildungseinrichtungen** (Ausnahme bei medizinischen Gründen und Sicherheitsgründen)
>> **Ableitung von besonders geschützten Daten anhand biometrischer Daten** (konkret: Ableitung von Informationen zur politischen Meinung, Gewerkschaftszugehörigkeit, Religion oder Weltanschauung, Rasse oder zum Sexualleben bzw. zur sexuellen Orientierung)
>> Verwendung **biometrischer Echtzeit-Fernidentifizierungssysteme** in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken (enge Ausnahmen vorgesehen)

Die Verbote knüpfen je nach Tatbestand an das Inverkehrbringen, die Inbetriebnahme oder die Verwendung des KI-Systems an, richten sich also auch an die Stellen, welche die KI-Systeme einsetzen, und nicht nur an die Anbieter entsprechender Systeme.

Mit der Einstufung von KI-Systemen als hochriskant und den insoweit geltenden Anforderungen befasst sich **Kapitel III** der KI-VO. Hier regeln zunächst die Artt. 8 bis 15 KI-VO die **Anforderungen an das Hochrisiko-KI-System** als solches. Diese Pflichten treffen naturgemäß primär die Anbieter betreffender Systeme.

Konkret beinhalten die „Anforderungen an das Hochrisiko-KI-System“ in Art. 8 ff. KI-VO, dass näher definierte Vorgaben zu den nachfolgend genannten Aspekten während des gesamten Lebenszyklus des KI-Systems eingehalten werden:[17]

>> **Risikomanagementsystem** als kontinuierlicher iterativer Prozess, der während des gesamten Lebenszyklus eines Hochrisiko-KI-Systems durchgeführt und aktualisiert wird (Art. 9 DS-GVO)
>> **Datenqualität** (Art. 10 KI-VO): Werden Hochrisiko-KI-Systeme mit Daten trainiert, müssen die Trainings-, Validierungs- und Testdatensätze gemäß Art. 10 KI-VO bestimmten Qualitätsanforderungen genügen.
>> **Dokumentation und Aufzeichnungspflichten** (Artt. 11 f. KI-VO)
>> **Transparenz und Bereitstellung von Informationen für Betreiber** der Hochrisiko-KI (Art. 13 KI-VO)
>> **Menschliche Aufsicht** (Art. 14 KI-VO)
>> **Genauigkeit, Robustheit und Cybersicherheit** (Art. 15 KI-VO)

Welche konkreten Pflichten Anbieter von Hochrisiko-KI-Systemen einhalten müssen, regelt Art. 16 KI-VO. Für bloße Betreiber gilt grundsätzlich der weniger umfassende Pflichtenkatalog in Art. 26 KI-VO. Wichtig ist allerdings, dass nach Art. 25 KI-VO ausnahmsweise (u.a.) auch Betreiber den Anbieterpflichten gemäß Art. 16 KI-VO unterfallen können.

Im Einzelnen ist Letzteres gemäß Art. 25 Abs. 1 KI-VO der Fall, sofern Betreiber

>> ein bereits in Verkehr gebrachtes oder in Betrieb genommenes Hochrisiko-KI-Sys-

17 Dazu im Einzelnen Schwartmann/Keber/Köhler/Zenner in LF KI-VO, 2. Teil 1. Kap. Rn. 266 ff.

tem mit ihrem Namen oder ihrer Handelsmarke versehen, unbeschadet vertraglicher Vereinbarungen, die eine andere Aufteilung der Pflichten vorsehen;

>> eine wesentliche Änderung an einem Hochrisiko-KI-System, das bereits in Verkehr gebracht oder in Betrieb genommen wurde, so vornehmen, dass es weiterhin ein Hochrisiko-KI-System bleibt;

>> die Zweckbestimmung eines KI-Systems, einschließlich eines KI-Systems mit allgemeinem Verwendungszweck, das nicht als hochriskant eingestuft wurde und bereits in Verkehr gebracht oder in Betrieb genommen wurde, so verändern, dass das betreffende KI-System zu einem Hochrisiko-KI-System wird.[18]

Eine allgemeine Pflicht für eine „Grundrechte-Folgenabschätzung für Hochrisiko-KI-Systeme“ wurde nicht eingeführt, sondern eine solche Pflicht ist nur für einen eng umgrenzten Bereich vorgesehen (vgl. Art. 27 Abs. 1 KI-VO), nämlich für staatliche Akteure bzw. private Einrichtungen, die öffentliche Dienste erbringen, sowie im Bereich der Privatwirtschaft für Fälle des Kreditscoring und KI-Systeme, die für die Risikobewertung und Preisbildung bei Kranken- und Lebensversicherungen eingesetzt werden.

Kapitel IV der KI-VO (Art. 50) enthält die bereits angesprochenen **Transparenzvorgaben** für Anbieter und Nutzer von KI-Systemen, welche für die direkte Interaktion mit natürlichen Personen bestimmt sind, etwa Chatbots, bzw. von solchen KI-Systemen, die Audio-, Bild-, Video- oder Textinhalte erzeugen.[19] Diese Pflichten bestehen unabhängig davon, welche Risiken mit dem KI-System ansonsten einhergehen. Denn aus Sicht des Verordnungsgebers sind KI-Systeme im vorbeschriebenen Sinne gewisse Risiken bereits immanent, besonders in Bezug auf Identitätsbetrug oder Täuschung (vgl. Erwägungsgrund 132 KI-VO). Mit den Transparenzvorgaben will der Verordnungsgeber diesen Risiken begegnen.

Kapitel V der KI-VO (Artt. 51 ff.) enthält besondere **Vorgaben zu KI-Modellen mit allgemeinem Verwendungszweck (“General Purpose Artificial Intelligence - GPAI”)**.[20] Gemeint sind KI-Modelle, welche eine erhebliche allgemeine Verwendbarkeit aufweisen und in der Lage sind, unabhängig von der Art und Weise des Inverkehrbringens ein breites Spektrum unterschiedlicher Aufgaben kompetent zu erfüllen, und die in eine Vielzahl nachgelagerter Systeme oder Anwendungen integriert werden können (Art. 3 Nr. 63 KI-VO). Nicht erfasst sind KI-Modelle, welche vor ihrer Markteinführung für Forschungs- und Entwicklungstätigkeiten oder die Konzipierung von Prototypen verwendet werden. Die Regulierung von GPAI war einer der umstrittensten Punkte im Rahmen des Gesetzgebungsverfahrens zur KI-VO. Diskutiert wurde u.a., ob GPAI-Modelle nicht generell als hochriskant eingestuft werden sollten. Dies ist im Ergebnis jedoch nicht geschehen. Vielmehr wurde eine neue Unterkategorie vorgesehen, nämlich diejenige der „GPAI-Modelle mit systemischem Risiko“. Letztere unterliegen im Verhältnis zu GPAI-Modellen ohne ein solches systemisches Risiko strengeren Auflagen. Entscheidend für die Einordnung als systemisch riskant ist, mit welcher Gesamtrechenleistung das System trainiert wurde. Hintergrund hierfür ist, dass Modelle tendenziell umso leistungsfähiger sind, je höher die Gesamtrechenleistung im Rahmen des Trainings war. Beispiel für GPAI-Modelle mit systemischem Risiko ist

18 Dazu Zenner/Schwartmann/Hansen in LF KI-VO, 2. Teil 1. Kap. Rn. 513 ff.

19 Dazu Kremer/Haar in LF KI-VO 2. Teil 1. Kap. Rn. 450 ff.

20 Dazu Zenner/Schwartmann/Hansen in LF KI-VO, 2. Teil 1. Kap. Rn. 487 ff.

etwa das GPT-4 Modell von OpenAI.[21] Relevant sind die Regelungen der Artt. 51 ff. primär für die **Anbieter von GPAI**.

Kapitel VI der KI-VO (Artt. 57 bis 63) enthält **Bestimmungen zur „Innovationsförderung"**.[22]

Kapitel VII (Artt. 64 bis 70) regelt unter dem Titel **„Governance"** die Um- und Durchsetzung der KI-VO.[23] Neben dem zentralen und für die Durchsetzung der GPAI[24]-Regelungen zuständigen **EU AI Office** werden folgende weitere Instanzen eingeführt: das „KI-Gremium" (Art. 65 KI-VO), das Beratungsforum (Art. 67 KI-VO) sowie das wissenschaftliche Gremium unabhängiger Sachverständiger (Art. 68 KI-VO).

Kapitel VIII (Art. 71) regelt die Errichtung und Führung einer **EU-Datenbank für Hochrisiko-KI-Systeme**.

Die weiteren Kapitel enthalten Informationen zu folgenden Bereichen:

>> **Kapitel IX** (Artt. 72 bis 94): **Beobachtung nach dem Inverkehrbringen, Informationsaustausch, Marktüberwachung**
>> **Kapitel X** (Artt. 95 und 96): **Verhaltenskodizes und Leitlinien**
>> **Kapitel XI** (Artt. 97 und 98): **Übertragung von Befugnissen und Ausschussverfahren**
>> **Kapitel XII** (Artt. 99 bis 101): **Sanktionen**
>> **Kapitel XIII** (Artt. 102 ff.): **Schlussbestimmungen**

V. KI und Datenschutz

1. Erfordernis einer Rechtsgrundlage stattfindender personenbezogener Datenverarbeitungen

Sofern im Zusammenhang mit KI-Systemen personenbezogene Daten verarbeitet werden, ist die DS-GVO zu beachten.[25] Zu einer entsprechenden Verarbeitung personenbezogener Daten kann es etwa kommen, weil im Rahmen des Trainings der KI auch personenbezogene Informationen verwendet werden oder aber, weil im Rahmen des späteren KI-Einsatzes personenbezogene Daten in das KI-System eingegeben werden.

Nach der DS-GVO bedürfen personenbezogene Datenverarbeitungen stets einer entsprechenden Rechtsgrundlage, vgl. Erwägungsgrund 40 DS-GVO, wobei zu beachten ist, dass die DS-GVO keine speziellen, explizit auf KI-Systeme zugeschnittenen Regelungen enthält. Für Datenverarbeitungen im Zusammenhang mit KI sind also die allgemeinen Rechtgrundlagen der DS-GVO heranzuziehen, also insbes. Art. 6 Abs. 1 lit. b) (Verarbeitungen im Zusammenhang mit einem Vertrag), Art. 6 Abs. 1 lit. f) (Verarbeitungen zur Wahrung berechtigter Interessen nach entsprechender Abwägung) und Art. 6 Abs. 1 lit. a) DS-GVO (Verarbeitung auf Basis einer Einwilligung der betroffenen Person).

Sofern im Zusammenhang mit KI besondere Arten personenbezogener Daten (Art. 9 Abs. 1 DS-GVO) verarbeitet werden, z.B. Gesundheitsdaten, sind – die im Verhältnis zu Art. 6 DS-GVO engeren Vorgaben – aus Art. 9 DS-GVO zu beachten. Insbesondere können Daten nach Art. 9 DS-GVO nicht auf Basis einer reinen Interessenabwägung verarbeitet werden.

Werden **Beschäftigtendaten** im Rahmen von KI verarbeitet, ist, sofern die Verarbeitung im Rahmen der Zwecke des Beschäftigungs-

21 https://ec.europa.eu/commission/presscorner/detail/de/QANDA_21_1683.
22 Dazu Keber/Hansen/Nägele in LF KI-VO, 2. Teil 1. Kap. Rn. 540 ff.
23 Dazu Schwartmann/Köhler in LF KI-VO, 3. Teil 1. Kap. Rn. 1 ff.
24 General Purpose AI, vgl. dazu Kapitel V (S. 10).
25 Zu KI und Datenschutz ausführlich Schwartmann/Keber/Zenner in LF KI-VO, 2. Teil 3. Kap.

verhältnisses erfolgt, Maßstab für die Zulässigkeit der Datenverarbeitung ist § 26 Abs. 1 S. 1 BDSG bzw. – dessen Europarechtswidrigkeit unterstellt[26] – Art. 6 Abs. 1 lit. b) DS-GVO. Für sog. „beschäftigungsfremde" Zwecke kommt ggf. ein Rückgriff auf Art. 6 Abs. 1 lit. f) DS-GVO als Rechtsgrundlage für die Datenverarbeitung in Betracht.[27] Auch eine Einwilligung des Beschäftigten kommt als denkbare Rechtsgrundlage in Betracht, allerdings bedarf es insoweit stets der besonderen Prüfung der Freiwilligkeit der Erklärung (vgl. § 26 Abs. 2 BDSG).

2. Weitere Grundsätze der Datenverarbeitung, insbes. Transparenz und bes. Pflichten im Falle automatisierter Einzelentscheidungen (Art. 22 DS-GVO)

Neben dem Prinzip der Rechtmäßigkeit der Datenverarbeitung (Art. 5 Abs. 1 lit. a) DS-GVO), müssen auch die anderen **Grundsätze für die Verarbeitung personenbezogener Daten** aus Art. 5 Abs. 1 DS-GVO beim KI-Einsatz nicht nur eingehalten werden, sondern die Einhaltung der Grundsätze muss vom Verantwortlichen auch entsprechend nachgewiesen werden können (Art. 5 Abs. 2 DS-GVO, sog. **Rechenschaftspflicht**). Praktisch bedeutsam wird in diesem Zusammenhang u.a. das Prinzip der **Transparenz** der Datenverarbeitung (Art. 5 Abs. 1 lit. a) DS-GVO), welches in Artt. 12 ff. DS-GVO näher konkretisiert ist.

Erfolgt im konkreten Fall eine **automatisierte Entscheidungsfindung** einschließlich Profiling **nach Art. 22 Abs. 1 und 4 DS-GVO**, so ist hierüber nach Art. 13 Abs. 2 lit. f) DS-GVO (bzw. Art. 14 Abs. 2 lit. g) DS-GVO) zu informieren. Zudem sind in diesem Fall „aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person" mitzuteilen. Es muss sich insofern um einen Fall handeln, in dem eine automatisierte Einzelentscheidung bzw. ein Profiling nach Art. 22 DS-GVO ausnahmsweise zulässig ist.

Gemäß Art. 22 DS-GVO gilt, dass automatisierte Einzelentscheidungen, sofern sie rechtliche Wirkung entfalten oder in ähnlicher Weise erheblich beeinträchtigend sind, **grundsätzlich verboten** sind. Natürliche Personen sollen nicht zum „Objekt" maschineller Entscheidungen werden, so die Intention hinter dem prinzipiellen Verbot.[28]

Das dargestellte prinzipielle Verbot automatisierter Einzelentscheidungen gilt lediglich dann nicht (vgl. Art. 22 Abs. 2 DS-GVO), wenn die Entscheidung

>> für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist (lit. a)),
>> aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten (lit. b)) oder
>> mit ausdrücklicher Einwilligung der betroffenen Person erfolgt (lit. c)).[29]

In den in lit. a) und c) genannten Fällen muss der Verantwortliche **angemessene Maßnahmen** treffen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren, wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gehört (Art. 22 Abs. 3 DS-GVO). Die **Information über die Rechte nach Art. 22 Abs. 3 DS-GVO** sollte sinnvollerweise mit den

26 Vgl. hierzu https://www.gdd.de/deutschland-gesetze/konsequenzen-der-eugh-entscheidung/
27 Schmidt/Thüsing in Schwartmann/Jaspers/Thüsing/Kugelmann, HK-DS-GVO/BDSG (4. Aufl. im Erscheinen), § 26 BDSG Rn. 39
28 Hessel/Dillschneider, RDi 2023, 458 (463).
29 Betrifft die Entscheidung Datenkategorien i.S.v. Art. 9 Abs. 1 DS-GVO, so muss der Verantwortliche zudem die Einhaltung der Bedingungen von Art. 22 Abs. 4 DS-GVO sicherstellen.

bereits angesprochenen **Informationen nach Art. 13 Abs. 2 lit. f) bzw. Art. 14 Abs. 2 lit. g) DS-GVO** verbunden werden[30] und nötigenfalls wiederholt werden, sobald es konkret zu einer beeinträchtigenden automatisierten Einzelentscheidung kommt.

Verantwortliche, die eine KI-Anwendung nicht selbst entwickeln, müssen darauf achten, vom Anbieter die notwendigen Informationen zu bekommen, um den bestehenden Transparenzpflichten nachkommen zu können. [31]

Die datenschutzrechtlichen Informationspflichten und nach der KI-VO bestehende Transparenzpflichten[32] sind unabhängig voneinander zu beachten, überschneiden sich aber in ihrem Informationsgehalt. In beiden Fällen geht es darum zu vermitteln, dass eine Maschine im Verhältnis zum Betroffenen agiert.

3. Datenschutz-Folgenabschätzung (Art. 35 DS-GV0)

Gemäß Art. 35 DS-GVO ist für besonders risikobehaftete Datenverarbeitungsvorgänge eine sog. Datenschutz-Folgenabschätzung durchzuführen. Bei dieser handelt es sich um eine präventive Überprüfung der möglichen Folgen der Datenverarbeitungsvorgänge für den Einzelnen, um anschließend risikominimierende Abhilfemaßnahmen auszuwählen und zu implementieren.[33] Ein Risiko, das eine Datenschutz-Folgenabschätzung erforderlich macht, kann sich nach dem expliziten Wortlaut von Art. 35 Abs. 1 DS-GVO „insbesondere bei Verwendung neuer Technologien“ ergeben.

Sofern KI zum Einsatz kommt und eine Verarbeitung personenbezogener Daten in diesem Zusammenhang nicht ausgeschlossen ist, wird es insofern regelmäßig der Durchführung einer Datenschutz-Folgenabschätzung bedürfen. [34]

Hilfestellung bei der Risikobeurteilung kann dabei etwa das nachfolgende Angebot der französischen Aufsichtsbehörde CNIL leisten:

>> CNIL, „Self-assessment guide for artificial intelligence (AI) systems“, abrufbar unter https://www.cnil.fr/en/self-assessment-guide-artificial-intelligence-ai-systems

4. Datenschutzrechtliche Verantwortlichkeit der Beteiligten beim Einsatz von KI

Weiter stellt sich beim Einsatz von KI-Systemen häufig die Frage nach der datenschutzrechtlichen Verantwortlichkeit beteiligter Akteure. Neben dem das KI-System einsetzenden Unternehmen sind in der Praxis typischerweise dessen Mitarbeiter/-innen als Nutzer und der Anbieter der KI am Einsatz beteiligt. Entscheidend für die Beurteilung der datenschutzrechtlichen Verantwortlichkeiten ist dabei stets die Ausgestaltung im konkreten Einzelfall.

Wird die KI-Anwendung auf eigenen Unternehmensservern zu ausschließlich eigenen Zwecken betrieben, so ist das Unternehmen regelmäßig datenschutzrechtlich **allein Ver-**

30 Gola/Heckmann/Schulz, 3. Aufl. 2022, DS-GVO Art. 22 Rn. 34.
31 DSK, Orientierungshilfe „Künstliche Intelligenz und Datenschutz“, Vers. 1.0, Rn. 21.
32 Vgl. unter II.
33 Ferik in Schwartmann/Jaspers/Thüsing/Kugelmann, HK-DS-GVO/BDSG (4 Aufl. im Erscheinen) Art. 35 DS-GVO Rn. 34
34 Vgl. etwa Kühling/Buchner/Jandt, 4. Aufl. 2024, DS-GVO Art. 35 Rn. 8; Schürmann, ZD 2022, 316; DSK, Orientierungshilfe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 06.05.2024 „Künstliche Intelligenz und Datenschutz“ (Vers. 1.0), Rn. 39.

antwortlicher i.S.v. Art. 4 Nr. 7 DS-GVO.[35]

Eine **gemeinsame Verantwortlichkeit gemäß Art. 26 DS-GVO** kommt insbes. dann in Betracht, wenn der Hersteller parallel zum Einsatz der KI ein „permanentes Monitoring" zum Zwecke der Kontrolle bzw. Weiterentwicklung der KI betreibt.[36] Die beteiligten Stellen haben in letzterem Fall gemäß Art. 26 Abs. 1 S. 2 DS-GVO in einer Vereinbarung in transparenter Form festzulegen, wer von ihnen welchen Verpflichtungen aus der DS-GVO nachkommt, insbes. der Erfüllung der Betroffenenrechte und der Informationspflichten gemäß Artt. 13 f. DS-GVO. Im Zusammenhang mit dem Einsatz von KI können schließlich auch **Auftragsverarbeitungsverhältnisse (Art. 28 DS-GVO)** begründet werden, z.B., wenn ein KI-System cloudbasiert betrieben wird.[37] Prinzipiell kann eine entsprechende Cloudlösung dabei auch durch den KI-Hersteller selbst angeboten werden.

Wichtig ist, dass eine Auftragsverarbeitung nur dann vorliegt, wenn personenbezogene Daten rein weisungsgebunden nach den Vorgaben des Auftraggebers verarbeitet werden. Sobald der Auftragnehmer Daten zumindest auch für eigene Zwecke verwendet, z.B. zu Analysezwecken, sind die Grenzen der Auftragsverarbeitung überschritten.

5. Sonstige Datenschutzaspekte

Weitere Gesichtspunkte, die beim KI-Einsatz aus Datenschutzsicht relevant werden können, sind etwa die Gewährleistung der Einhaltung der **Betroffenenrechte nach Artt. 12 ff. DS-GVO**, insbes. des Rechts auf Auskunft (Art. 15 DS-GVO), und die Wahrung der **Vorschriften zum Drittlandtransfer (Artt. 44 ff. DS-GVO)**, sofern im Zusammenhang mit dem KI-Einsatz personenbezogene Daten in Bereiche außerhalb der EU/des EWR transferiert werden. Der Verantwortliche sollte sich vorab auf die Erfüllung der Betroffenenrechte vorbereiten und, soweit möglich, TOMs zur effizienten Umsetzung der Vorgaben implementieren.[38]

VI. Nationale Gesetzgebung

Auf nationaler Ebene gibt es bisher keine Regelungen, welche den Umgang mit KI speziell regeln. Nach Inkrafttreten der geplanten EU-Richtlinie über die Haftung für KI[39] wird der deutsche Gesetzgeber diese jedoch in nationales Recht umzusetzen haben.

VII. Weiterführende Hinweise zur KI-VO

>> EU-Kommission, Künstliche Intelligenz – Fragen und Antworten (Stand: 12.12.2023), https://ec.europa.eu/commission/presscorner/detail/de/QANDA_21_1683

>> DSK, Orientierungshilfe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 06.05.2024 „Künstliche Intelligenz und Datenschutz" (Vers. 1.0), https://www.datenschutzkonferenz-online.de/media/oh/20240506_DSK_Orientierungshilfe_KI_und_Datenschutz.pdf

>> LfDI BW, Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz, Diskussionspapier, Vers. 1.0 vom 07.11.2023, https://www.baden-wuerttemberg.datenschutz.de/rechtsgrundlagen-datenschutz-ki/

35 DSK, Orientierungshilfe „Künstliche Intelligenz und Datenschutz", Vers. 1.0, Rn. 32.
36 Hoeren/Sieber/Holznagel, MMR-HdB, Teil 29 Rn. 17, beck-online.
37 DSK, Orientierungshilfe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 06.05.2024 „Künstliche Intelligenz und Datenschutz", Rn. 32.
38 Ashkar, ZD 2023, 523 (528).
39 Vgl. hierzu im Einzelnen Abschnitt A. IV. in dieser Praxishilfe.

>> Kremer, Künstliche Intelligenz im Unternehmen und der Datenschutz: Kommentierte Checkliste für die betriebliche Praxis, RDV 2023, 281

>> Ashkar, Wesentliche Anforderungen der DS-GVO bei Einführung und Betrieb von KI-Anwendungen, ZD 2023, 523

C. Data Act (DA)

I. Inkrafttreten und Geltung

Die „Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung“ (kurz: Data Act) ist am 11. Januar 2024 in Kraft getreten und gilt nach einer 20-monatigen Übergangsfrist **ab dem 12. September 2025 als EU-weit direkt anwendbares Recht**.

II. Ziele des Data Act und Anwendungsbereich

Ansatzpunkt des DA ist der Umstand, dass nach Auffassung der EU-Kommission bisher in der europäischen Wirtschaft der Wert von Daten nicht in ausreichendem Maße ausgeschöpft wurde.[40] Mittels des DA soll daher ein harmonisierter Rahmen eingeführt werden, in dem festgelegt ist, wer unter welchen Bedingungen berechtigt ist, Zugriff auf Daten zu erhalten, die im Zusammenhang mit vernetzten Produkten oder verbundenen Diensten in Europa erzeugt werden.[41] Mit Blick auf den DA müssen vernetzte Produkte so konzipiert und hergestellt werden, dass auf die erzeugten Daten einfach und sicher zugegriffen werden kann und diese ebenso einfach weiterverwendet und geteilt werden können.[42]

Datenzugangsberechtigt nach dem DA sind die Nutzer/-innen vernetzter Produkte oder verbundener Dienste.

„Vernetzte Produkte“ sind nach Art. 2 Nr. 5 DA Gegenstände, die Daten über ihre Nutzung oder Umgebung generieren und Produktdaten übermitteln können. Hauptanwendungsfall sind insofern **Geräte aus dem Bereich des Internets der Dinge** („Internet of Things - IoT“-Geräte), wie z.B. smarte Staubsauger oder Kühlschränke oder auch moderne vernetzte KFZ („Connected Car“). Auch industrielle Maschinen und Anlagen können vernetzte Produkte im Sinne des DA darstellen (vgl. Erwägungsgrund 14 S. 3 DA). „Verbundene Dienste“ sind nach Art. 2 Nr. 6 DA digitale Dienste, welche die Funktionsfähigkeit eines vernetzten Produkts erst ermöglichen, also z.B. die Software für die Smart Watch oder das vernetzte KFZ. **Rein digitale Dienstleistungen** fallen nicht in den Anwendungsbereich des DA und auch reine elektronische Kommunikationsdienste, wie z.B. der Internetzugang, sind **nicht erfasst**. Gegenstand des DA sind physische Gegenstände mit einer digitalen Komponente.

Wichtig: Der DA betrifft Daten, die bei der Nutzung von vernetzten Produkten oder verbundenen Diensten erzeugt werden, unabhängig von ihrem Personenbezug. Der Anwendungsbereich des DA ist also weiter als derjenige der DS-GVO. Zum Verhältnis zwischen den Vorgaben des DA und denjenigen der DS-GVO vgl. unter V.

40 EU-Kommission, Datengesetz – Fragen und Antworten, Stand: 28.06.2023.
41 EU-Kommission, Datengesetz – Fragen und Antworten, Stand: 28.06.2023.
42 https://digital-strategy.ec.europa.eu/de/policies/data-act.

Der DA ist eine sektorübergreifende Gesetzgebung, d.h., er legt Grundsätze und Leitlinien fest, die für alle Sektoren gelten. Geschaffen wird ein „horizontaler Minimalstandard für weitergehende sektorale Lösungen“[43]. Bestehende Datenzugangsverpflichtungen ändert die Verordnung nicht, doch sollen künftige Rechtsvorschriften mit ihren Grundsätzen in Einklang stehen.

Die Regelungen des DA stehen in engem Zusammenhang mit denjenigen des **Data Governance Act (DGA)**.[44] Während der DGA Prozesse und Strukturen für einen freiwilligen Datenaustausch vorsieht, soll der DA für eine gerechte Verteilung des Datenwertes sorgen, indem Regeln für den Zugriff auf und die Nutzung von Daten innerhalb der europäischen Datenwirtschaft aufgestellt werden.[45] Gemeinsam sollen DA und DGA einen zuverlässigen und sicheren Zugang zu Daten ermöglichen und die Datennutzung in wichtigen Wirtschaftssektoren und Bereichen von öffentlichem Interesse fördern, wodurch im Sinne von Wirtschaft und Gesellschaft zur Schaffung eines EU-Datenbinnenmarkts beigetragen wird.[46]

III. Adressaten

Gemäß Art. 1 Abs. 3 DA gilt die Verordnung für:

>> **Hersteller vernetzter Produkte**, die in der Union in Verkehr gebracht werden, und Anbieter verbundener Dienste, unabhängig vom Ort der Niederlassung dieser Hersteller oder Anbieter;
>> **die Nutzer der genannten vernetzten Produkte oder verbundenen Dienste in der Union**;
>> **Dateninhaber**, unabhängig vom Ort ihrer Niederlassung, die Datenempfängern in der Union Daten bereitstellen;

„Dateninhaber“ ist gemäß Art. 2 Nr. 13 DA jede natürliche oder juristische Person, die […] berechtigt oder verpflichtet ist, Daten – soweit vertraglich vereinbart, auch Produktdaten oder verbundene Dienstdaten – zu nutzen und bereitzustellen, die sie während der Erbringung eines verbundenen Dienstes abgerufen oder generiert hat.

>> **Datenempfänger** in der Union, denen Daten bereitgestellt werden;
>> **öffentliche Stellen**, die Kommission, die Europäische Zentralbank und Einrichtungen der Union, die von Dateninhabern verlangen, Daten bereitzustellen, soweit eine außergewöhnliche Notwendigkeit der Nutzung dieser Daten zur Wahrnehmung einer speziellen Aufgabe im öffentlichen Interesse besteht, sowie die Dateninhaber, die solche Daten auf ein solches Verlangen hin bereitstellen;
>> **Anbieter von Datenverarbeitungsdiensten**, unabhängig vom Ort ihrer Niederlassung, die Kunden in der Union solche Dienste anbieten;
>> **Teilnehmer an Datenräumen und Anbieter von Anwendungen**, die intelligente Verträge verwenden, und Personen, deren gewerbliche, geschäftliche oder berufliche Tätigkeit die Einführung intelligenter Verträge für andere im Zusammenhang mit der Durchführung einer Vereinbarung umfasst.

43 Podszun/Pfeifer, GRUR 2022, 953 (961).
44 Zum Data Governance Act vgl. auch Abschnitt D in dieser Praxishilfe.
45 https://digital-strategy.ec.europa.eu/de/policies/data-act.
46 https://digital-strategy.ec.europa.eu/de/policies/data-act.

Die Vorgaben des DA sind für Unternehmen nicht nur deshalb von Bedeutung, weil sie ggf. nach dem DA auf Datenzugang in Anspruch genommen werden können, sondern auch als potenziell anspruchsberechtigte Nutzer im Sinne des DA, sofern vernetzte Produkte oder verbundene Dienste verwendet werden.

IV. Wesentliche Inhalte des DA

Kapitel I des DA enthält allgemeine Regelungen zum Gegenstand und **Anwendungsbereich** der VO (Art. 1) **sowie** den **Begriffsbestimmungen** (Art. 2).

Kapitel II (Artt. 3 bis 7 DA) enthält **Vorgaben zur Datenweitergabe von Unternehmen an Verbraucher (B2C) sowie zwischen Unternehmen (B2B)**.

Ausgangspunkt ist dabei der **direkte Datenzugang des Nutzers gemäß Art. 3 DA**. Gemäß Art. 3 Abs. 1 DA sind vernetzte Produkte so zu konzipieren und herzustellen und verbundene Dienste so zu konzipieren und zu erbringen, *„dass die **Produktdaten und** verbundenen **Dienstdaten […] standardmäßig für den Nutzer** einfach, sicher, unentgeltlich in einem umfassenden, strukturierten, gängigen und maschinenlesbaren Format und, soweit relevant und technisch durchführbar, **direkt zugänglich** sind“*.

Soweit der Nutzer nicht direkt vom vernetzten Produkt oder verbundenen Dienst aus auf die Daten zugreifen kann, hat er nach Art. 4 Abs. 1 DA einen Anspruch darauf, „ohne Weiteres verfügbare Daten“ vom Dateninhaber bereitgestellt zu erhalten (**Bereitstellungsanspruch des Nutzers gegen den Dateninhaber**). Die Bereitstellung hat unverzüglich, einfach, sicher, unentgeltlich, in einem umfassenden, gängigen und maschinenlesbaren Format und – falls relevant und technisch durchführbar – in der gleichen Qualität wie für den Dateninhaber kontinuierlich und in Echtzeit zu erfolgen. Auf Verlangen des Nutzers hat die Bereitstellung auf elektronischem Weg zu erfolgen, sofern technisch möglich.

In Art. 5 DA finden sich Regelungen zum **Recht des Nutzers auf Weitergabe von Daten an Dritte**. Daten, die aufgrund von Art. 4 Abs. 1 DA dem Nutzer selbst zur Verfügung zu stellen wären, sind auf dessen Verlangen Dritten bereitzustellen. Der Dritte darf die bereitgestellten Daten nur gemäß den Bedingungen verarbeiten, die er und der Nutzer, auf dessen Verlangen der Dritte die Daten erhält, vereinbart haben (Art. 6 Abs. 1 DA). Über entsprechende Detailregelungen in Artt. 5 f. DA wird dabei sichergestellt, dass „Gatekeeper“ im Sinne des DMA[47] nicht über den DA an Daten kommen können.

Die Pflichten bzw. Rechte aus Artt. 3 bis 5 DA beziehen sich neben den Produkt- bzw. Dienstdaten jeweils auch auf die zur „Auslegung und Nutzung dieser Daten erforderlichen **Metadaten**“.

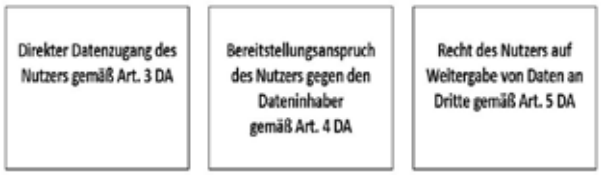

Abbildung: Ausgestaltung des Datenzugangs nach dem DA

In Art. 3 Abs. 2 und 3 DA sind schließlich **umfassende vorvertragliche Informationspflichten** mit Blick auf die stattfindende Datenverarbeitung vorgesehen, sofern Kauf-, Miet- oder Leasingverträge bezogen auf vernetzte Produkte geschlossen werden bzw. Verträge für die Erbringung von verbundenen Diensten.

47 Zum Begriff des „Gatekeepers“ vgl. Abschnitt F. II. in dieser Praxishilfe.

Kapitel III (Artt. 8 bis 12 DA) regelt die **Pflichten der Dateninhaber, die verpflichtet sind, Daten bereitzustellen**, inkl. Gegenleistungen für die Datenbereitstellung im B2B-Bereich (Art. 9 DA). Zentral im Rahmen des Kapitel III ist die Pflicht aus Art. 8 Abs. 1 DA, wonach ein Dateninhaber, wenn er zur Bereitstellung von Daten verpflichtet ist, die Einhaltung der sog. FRAND-Grundsätze zu beachten hat. Der Zugang muss also zu Bedingungen gewährleistet werden, die „fair, reasonable and non-discriminatory" sind.

Kapitel IV (Art. 13 DA) enthält **Regelungen zu missbräuchlichen Vertragsklauseln** in Bezug auf den Datenzugang und die Datennutzung zwischen Unternehmen. Gemäß Art. 13 Abs. 3 DA sind Vertragsklauseln missbräuchlich, wenn ihre Anwendung eine grobe Abweichung von der guten Geschäftspraxis bei Datenzugang und Datennutzung darstellt oder gegen das Gebot von Treu und Glauben verstößt.

Kapitel V (Artt. 14 bis 22 DA) enthält spezielle Vorgaben zur **Bereitstellung von Daten gegenüber öffentlichen Stellen**. Öffentliche Stellen sollen in bestimmten Situationen von außergewöhnlichem Bedarf mehr faktengestützte Entscheidungen treffen können, indem sie auf bestimmte Daten des Privatsektors zugreifen.[48]

Kapitel VI (Artt. 23 bis 31 DA) regelt den **Wechsel zwischen Datenverarbeitungsdiensten**: Anbieter von Cloud- und Edge-Computing-Diensten müssen danach Mindestanforderungen erfüllen, um die Interoperabilität zu erleichtern und den Wechsel zu ermöglichen.[49]

Kapitel VII (Art. 32 DA) befasst sich mit dem **staatlichen Zugang zu Daten sowie staatlichen Übermittlungen im internationalen Umfeld**. Mittels der getroffenen Regelungen sollen Daten, die in der EU gespeichert sind, vor unrechtmäßigen Zugriffsanfragen ausländischer Regierungen geschützt werden.[50]

Kapitel VIII (Artt. 33 bis 36 DA) enthält Bestimmungen zur **Interoperabilität** für Teilnehmer an Datenräumen.

Kapitel IX (Artt. 37 bis 42 DA) ist **Anwendung und Durchsetzung des DA** gewidmet. Die Mitgliedstaaten müssen eine zuständige Behörde oder mehrere zuständige Behörden benennen, um die Vorgaben des DA zu überwachen und durchzusetzen. Sofern mehrere Behörden benannt werden, bedarf es der Benennung eines „Datenschutzkoordinators" als zentrale Anlaufstelle.

Kapitel X (Art. 43 DA) regelt das **Verhältnis zur Richtlinie 96/9/EG** und das **Kapitel XI** (Artt. 44 ff. DS-GVO) enthält **Schlussbestimmungen**.

V. Verhältnis zum Datenschutzrecht

Der DA erfasst Daten, die bei der Nutzung von vernetzten Produkten oder verbundenen Diensten erzeugt werden, unabhängig von einem Personenbezug.

Soweit Datenzugangsansprüche gemäß DA sich auf Daten mit Personenbezug beziehen, stellt sich die Frage nach dem Verhältnis zu den diesbezüglichen Vorgaben der DS-GVO. Der Verordnungsgeber hat das potenzielle Konfliktpotenzial zwischen beiden Regelungswerken erkannt und in Art. 1 Abs. 5 DA hierzu eine Regelung vorgesehen. Art. 1 Abs. 5 S. 1 und 3 DA bestimmen insofern, dass der Data Act „unbeschadet" der unionsrechtlichen wie nationalen Datenschutzbestimmungen gilt und im Falle eines Widerspruchs die Regelungen des Datenschutzrechts Vorrang genießen.

48 https://digital-strategy.ec.europa.eu/de/factpages/data-act-explained.
49 https://digital-strategy.ec.europa.eu/de/factpages/data-act-explained.
50 https://digital-strategy.ec.europa.eu/de/factpages/data-act-explained.

Mit anderen Worten: Verantwortliche, die Ansprüchen nach dem DA ausgesetzt sind, müssen vor Erfüllung der Ansprüche prüfen, ob hierdurch personenbezogene Daten betroffen sind. In entsprechenden Fällen sind als zusätzlicher Filter vor Erfüllung des Anspruchs die DS-GVO-Vorgaben zu beachten. Schwierigkeiten können sich insbes. dann ergeben, wenn auch Daten von Dritten und nicht nur Daten derjenigen Person betroffen sind, die den Zugangsanspruch nach dem DA geltend macht.[51]

Näher konkretisiert wird das Verhältnis von DA und DS-GVO noch in Erwägungsgrund 7 DA, der u.a. Folgendes besagt: *„Keine Bestimmung dieser Verordnung sollte dahingehend angewandt oder ausgelegt werden, dass das Recht auf den Schutz personenbezogener Daten oder das Recht auf Privatsphäre und Vertraulichkeit der Kommunikation abgeschwächt oder eingeschränkt wird. Jegliche Verarbeitung personenbezogener Daten nach dieser Verordnung sollte dem Datenschutzrecht der Union entsprechen, einschließlich dem Erfordernis einer gültigen Rechtsgrundlage für die Verarbeitung gemäß Art. 6 der Verordnung (EU) 2016/679[52] und ggf. den Bedingungen des Art. 9 der genannten Verordnung und des Art. 5 Abs. 3 der Richtlinie 2002/58/EG[53]. Die vorliegende Verordnung stellt keine Rechtsgrundlage für die Erhebung oder Generierung personenbezogener Daten durch den Dateninhaber dar.“*

Im Anwendungsbereich der DS-GVO ergänzen die Rechte aus Kapitel II des DA die Rechte nach der DS-GVO auf Auskunft (Art. 15) und Datenübertragbarkeit (Art. 20). Dies besagt Art. 1 Abs. 5 S. 2 DA.

VI. Nationale Regelungen

Auf nationaler Ebene gibt es bisher keine Regelungen bzw. Regelungsvorhaben, die den DA näher spezifizieren oder ausfüllen.

VII. Weiterführende Hinweise

>> EU-Kommission, Datengesetz – Fragen und Antworten, Stand: 28.06.2023 https://ec.europa.eu/commission/presscorner/detail/de/qanda_22_1114
>> Paal/Cornelius/Seeland, Ausgewählte Probleme des Data Act – insbesondere im Zusammenspiel mit der DS-GVO, RDV 2024, 5 ff.
>> Götz/Blöink, Datenvertrag: Lösungsansatz für das Spannungsfeld zwischen Data Act und DS-GVO, MMR 2024, 451

D. Data Governance Act

I. Inkrafttreten und Geltung

Der Data Governance Act (kurz: DGA) trat am 23. Juni 2022 in Kraft und gilt seit September 2023.

II. Ziele und Anwendungsbereich

Gemeinsam mit dem Data Act (DA) bildet der DGA eine zentrale Säule der EU-Datenstrategie mit dem Ziel, die **Wertschöpfung aus Daten** durch Schaffung entsprechender rechtlicher

51 Götz/Blöink, MMR 2024, 451 (455).
52 = DS-GVO.
53 = ePrivacy-Richtlinie.

Rahmenbedingungen zu fördern. Konkret zielt der DGA darauf, das Vertrauen in den Datenaustausch sowie die Mechanismen zur Erhöhung der Datenverfügbarkeit zu stärken und technische Hindernisse für die Weiterverwendung von Daten zu überwinden.[54] Zugleich unterstützt der DGA die **Entwicklung gemeinsamer europäischer Datenräume** in strategisch wichtigen Bereichen wie Gesundheit, Umwelt, Energie, Landwirtschaft, Mobilität, Finanzen, verarbeitende Industrie und öffentliche Verwaltung.[55] Es sollen mehr Daten verfügbar gemacht werden und der Datenaustausch zwischen Sektoren und EU-Ländern soll erleichtert werden, damit das Potenzial der Daten zum Nutzen der europäischen Bürger/-innen und Unternehmen besser ausgeschöpft werden kann.[56]

Vorangetrieben werden soll die Entwicklung vertrauenswürdiger Datenaustauschsysteme im Einzelnen durch folgende Maßnahmenpakete:[57]

>> **Erleichterung der Weiterverwendung bestimmter Daten des öffentlichen Sektors**, die nicht als offene Daten zur Verfügung gestellt werden können (Beispiel: Weiterverwendung von Gesundheitsdaten für Forschungszwecke, um Heilungen für seltene oder chronische Krankheiten zu finden)

>> Sicherstellung, dass **Datenintermediäre als vertrauenswürdige Organisatoren** für den Datenaustausch innerhalb der gemeinsamen europäischen Datenräume fungieren

>> Erleichterungen für Bürger/-innen und Unternehmen, ihre Daten zum Wohle der Gesellschaft zur Verfügung zu stellen (sog. **Datenaltruismus**)

>> **Erleichterung des Datenaustauschs, insbes. um eine sektor- und grenzübergreifende Nutzung von Daten zu ermöglichen** und die Suche nach den richtigen Daten für den richtigen Zweck zu ermöglichen

Der DGA richtet sich vor allem an öffentliche Stellen, Datenvermittlungsdienste und datenaltruistische Organisationen.

E. Digital Service Act

I. Inkrafttreten und Geltung

Seit dem 17. Februar 2024 gelten die an Online-Vermittler und Online-Plattformen gerichteten Vorschriften des Digital Services Act (kurz: DSA) vollumfassend und unmittelbar in den Mitgliedstaaten.[58]

II. Ziele und Anwendungsbereich[59]

Der DSA verfolgt zunächst das Ziel, Verbraucher/-innen und deren Grundrechte im Internet zu schützen. Insbes. sollen **illegale oder schädliche Online-Aktivitäten sowie die Verbreitung von Desinformation** verhindert werden. Darüber hinaus sollen Innovation, Wachstum und Wettbewerbsfähigkeit gefördert und die Expansion kleinerer Plattformen sowie von KMU und Start-ups erleichtert werden.

54 https://digital-strategy.ec.europa.eu/de/policies/data-governance-act.
55 https://digital-strategy.ec.europa.eu/de/policies/data-governance-act.
56 https://digital-strategy.ec.europa.eu/de/policies/data-governance-act.
57 https://digital-strategy.ec.europa.eu/de/policies/data-governance-act.

58 Für sog. sehr große Online-Plattformen und Online-Suchmaschinen mit mehr als 45 Millionen Nutzern in der EU (10 % der EU-Bevölkerung) waren die Vorschriften bereits seit Ende August 2023 zu beachten.
59 Die Ausführungen in diesem Abschnitt basieren auf den Informationen unter https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_de.

Adressaten des DSA sind Online-Vermittler und Online-Plattformen wie z.B. Onlinemarktplätze, soziale Netzwerke, Content-Sharing-Plattformen, App-Stores, Reise- und Unterkunftsportale. Die Pflichten der einzelnen Online-Unternehmen variieren je nach Rolle, Größe und Auswirkung im Online-Umfeld.

III. Ergänzende nationale Gesetzgebung

In Deutschland wird der DSA durch das „Digitale-Dienste-Gesetz (DDG)" ergänzt, welches am 14. Mai 2024 in Kraft getreten ist. Das DDG regelt insbes. die nationale Plattformaufsicht. Zuständig für die Überwachung, ob die Vorgaben des DSA eingehalten werden, und entsprechende Bußgelder bei Verstoß ist danach grundsätzlich eine unabhängige Koordinierungsstelle für digitale Dienste innerhalb der Bundesnetzagentur. Sofern Aufgaben der Koordinierungsstelle die DS-GVO betreffen, entscheidet diese im Benehmen mit der zuständigen Datenschutzaufsichtsbehörde (§ 19 Abs. 1 DDG). Sonderzuständigkeiten sieht das DDG für die Aufsicht im Bereich der Werbung und im Bereich des Jugendschutzes vor. Zuständige Behörde für die Durchsetzung von Art. 26 Abs. 3 und Art. 28 Abs. 2 und 3 DSA ist gemäß § 12 Abs. 3 DDG der/die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI). Konkret geht es um die Durchsetzung des Verbots, profilbasierte Werbung gegenüber Minderjährigen auszuspielen, sowie des Verbots, Werbung – auch gegenüber Erwachsenen – auszuspielen, wenn für die Profilbildung sog. besondere Kategorien personenbezogener Daten (Art. 9 Abs. 1 DS-GVO) verwendet wurden.

F. Digital Markets Act

I. Inkrafttreten und Geltung

Seit dem 2. Mai 2023 gilt der Digital Markets Act (DMA) unmittelbar in den Mitgliedstaaten der Union. Zur Einhaltung der Vorgaben des DMA sind Unternehmen aber erst verpflichtet, nachdem die EU-Kommission sie als sog. „Gatekeeper" im Sinne des DMA eingeordnet hat (vgl. dazu nachfolgend unter II.).

II. Ziele und Anwendungsbereich

Mit dem DMA wurde ein **Verhaltenskodex für große Digitalunternehmen** aufgestellt. Ziel ist die Ermöglichung von mehr Wettbewerb und Fairness seitens der großen digitalen Player. Diese sollen nicht länger allein die Spielregeln bestimmen können, indem sie z.B. Rankings ihre eigenen Angebote bevorzugen. Der DMA enthält Pflichten in Form von Geboten und Verboten, an die sich die ganz großen Digitalunternehmen im Geschäftsalltag halten müssen.[60]

Die Pflichten des DMA richten sich an Unternehmen, die von der EU-Kommission zuvor als sog. „Gatekeeper" (digitale Torwächter) eingestuft worden sind.

„Gatekeeper" sind große Online-Plattformen, die eine wichtige Schnittstelle zwischen Unternehmen und Verbrauchern bilden.[61] Sie besitzen die Macht, als privater Regelsetzer zu

60 Zu den Dos und Don'ts im Einzelnen vgl. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_de.
61 https://germany.representation.ec.europa.eu/news/gesetz-uber-digitale-markte-regeln-fur-digitale-torwachter-gelten-ab-heute-2023-05-02_de.

agieren und somit einen Engpass in der digitalen Wirtschaft zu schaffen.[62] Am 6. September 2023 hat die EU-Kommission erstmals sechs Gatekeeper benannt – **Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft**. Insgesamt wurden 22 Dienste benannt, die von diesen Gatekeepern bereitgestellt werden.[63]

III. Ergänzende nationale Gesetzgebung

Die Durchsetzung des DMA erfolgt grundsätzlich durch die EU-Kommission. Der DMA eröffnet den Mitgliedstaaten jedoch die Option, auch nationalen Wettbewerbsbehörden Befugnisse für eigene Ermittlungen im Hinblick auf mögliche Verstöße gegen den DMA einzuräumen, was in Deutschland im Rahmen der 11. Novelle des Gesetzes gegen Wettbewerbsbeschränkungen (GWB) erfolgt ist.[64] Zusätzlich wurde die private Rechtsdurchsetzung im Hinblick auf den DMA durch Anpassungen im GWB gestützt.

Der DMA gilt komplementär zum deutschen und europäischen Wettbewerbsrecht.

62 https://germany.representation.ec.europa.eu/news/gesetz-uber-digitale-markte-regeln-fur-digitale-torwachter-gelten-ab-heute-2023-05-02_de.
63 Vgl. zum gesamten Absatz unter https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en.
64 https://www.bundeskartellamt.de/DE/DigitalWirtschaft/RegelnDigitalwirtschaft/regelndigitalwirtschaft_node.html# („Wer setzt den DMA durch?").

G. NIS-2-Richtlinie

I. Inkrafttreten und Geltung

Die NIS-2-Richtlinie wurde am 27.12.2022 im Amtsblatt der EU veröffentlicht und ist am 16.01.2023 in Kraft getreten.

Die Richtlinie selbst ist für die Stellen in den Mitgliedstaaten nicht bindend. Die Mitgliedstaaten müssen die Richtlinie vielmehr noch innerhalb von 21 Monaten nach ihrem Inkrafttreten – also bis Oktober 2024 – in nationales Recht umsetzen. In Deutschland liegt hierzu seit Mai 2024 ein Referentenentwurf für ein „NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz" vor. [65]

II. Ziele und Anwendungsbereich der Vorgaben

Die NIS-2-Richtlinie ist Teil der europäischen Cybersicherheitsstrategie und aktualisiert im Jahr 2016 eingeführte Cybersicherheitsvorschriften der EU (NIS-1-Richtlinie). Durch Anpassung des Rechtsrahmens soll der zunehmenden Digitalisierung einerseits und einer sich entwickelnden Bedrohungslandschaft für Cybersicherheit andererseits Rechnung getragen werden.[66] Die zur Umsetzung der NIS-2-Richtlinie notwendigen nationalen Neuregelungen werden vor allem im BSI-Gesetz erfolgen. Zu den wesentlichen Änderungen durch die NIS-2-Richtlinie gehört die **Einführung von neuen Einrichtungskategorien, die im Bereich der Cybersicherheit erhöhte Anforderungen zu beachten haben**,

65 https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/nis2umsucg.html.
66 https://digital-strategy.ec.europa.eu/de/policies/nis2-directive.

konkret der Kategorien „besonders wichtige Einrichtungen“ und „wichtige Einrichtungen“. Damit ist eine signifikante Ausweitung der Verpflichteten verbunden. Die **bisherige Kategorie „KRITIS“** bleibt als zusätzliche Kategorie bestehen. Allerdings werden die bisherigen KRITIS-Betreiber, die Kritischen Infrastrukturen, durch NIS-2 zu „Betreibern kritischer Anlagen“. Erfasst werden durch Rechtsverordnung näher spezifizierte Anlagenarten in den Sektoren Energie, Transport und Verkehr, Finanz- und Versicherungswesen, Gesundheitswesen, Wasser, Ernährung, Informationstechnik und Telekommunikation, Weltraum und Siedlungsabfallentsorgung, sofern im Hinblick auf den Versorgungsgrad der Bevölkerung bestimmte Schwellenwerte überschritten werden.

Die durch die NIS-2-Richtlinie neu eingeführten **Kategorien der „besonders wichtigen Einrichtung“ bzw. „wichtigen Einrichtung“** sollen nach dem vorliegenden Referentenentwurf[67] in Form von Anlagen zum Gesetz definiert werden.[68] Zu den „wichtigen Einrichtungen“ zählen etwa Lebensmittelunternehmen, Post- und Kurierdienste oder Forschungseinrichtungen, sofern eine gewisse Größe überschritten wird. Entscheidend ist, ob das Unternehmen mindestens 50 Mitarbeiter beschäftigt oder einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro aufweist.

Die Verpflichtungen aufgrund der NIS-2-Richtlinie lassen sich grob in folgende drei Kategorien einordnen, nämlich erstens **Governance und Awareness**, zweitens **Risikomanagement** und drittens **Meldepflichten**, wobei die konkreten Pflichten danach variieren, ob es sich um eine „KRITIS“-Anlage, eine „besonders wichtige Einrichtung“ oder eine „wichtige Einrichtung“ handelt.

Für Verstöße sieht die NIS-2-Richtlinie deutlich stärkere **Sanktionen** vor als bislang. Der Bußgeldrahmen ist der DS-GVO nachempfunden, wobei im Einzelnen zwischen KRITIS, besonders wichtigen Einrichtungen und wichtigen Einrichtungen unterschieden wird. Neben Bußgeldern kommt ein Einschreiten der Aufsichtsbehörde (Bundesamt für Sicherheit in der Informationstechnik – BSI) sowie eine Haftung der Verantwortungsträger für Schäden aufgrund mangelhafter Cybersicherheit in Betracht.

Wichtig: Unternehmen müssen eigeninitiativ prüfen, ob sie durch NIS-2 betroffen sind. Dies ist umso relevanter, als unter die Vorgaben aufgrund von NIS-2 deutlich mehr Stellen fallen werden als dies auf Basis der ersten NIS-Richtlinie der Fall war.

H. Auswirkungen der EU-Datenstrategie auf den Datenschutzbeauftragten (DSB)

I. Ausgangspunkt – Aufgabenbereich des DSB und Vermeidung von Interessenkonflikten

Der EDSA hat angekündigt, sein Working Paper (WP) 243rev.01 zum Datenschutzbeauftragten[69] zu überarbeiten. Dabei sollen insbesondere Ergebnisse Berücksichtigung finden, welche sich im Rahmen der koordinierten Durchsetzungsmaßnahme ergeben haben, die der EDSA 2023 bezogen auf die Benennung und Position von Datenschutzbeauftragten durchgeführt hat. Nach den Ankündigungen des EDSA sollen zudem die neuen EU-Rechtsvorschriften im digitalen Bereich berücksichtigt werden wie die

67 https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwuerfe/CI1/NIS-2-RefE.pdf?__blob=publicationFile&v=5.
68 Vgl. S. 70 ff. des in der vorstehenden Fußnote verlinkten Entwurfs.

69 Das WP ist abrufbar über https://ec.europa.eu/newsroom/article29/items/612048.

KI-Verordnung, der Digital Services Act, der Digital Market Act und der Data Act. Es scheine, so der EDSA, dass Datenschutzbeauftragte einiger Organisationen im Rahmen dieser Gesetze intern Schlüsselrollen übernehmen. Solche neuen Rollen könnten zum einen das Risiko von Interessenkonflikten verstärken, so der EDSA. Zum anderen bestehe die Gefahr, dass der Amtsinhaber durch die neuen Aufgaben nicht mehr über die notwendigen zeitlichen Ressourcen für seine Aufgaben als Datenschutzbeauftragter verfügt. Entsprechend sieht auch das nationale BayLDA einen „klaren Anlass", die aufsichtsbehördlichen Prüfungen zu Aufgaben und Position von Datenschutzbeauftragten fortzuführen und ggf. zu vertiefen. Die Aufsichtsbehörde in Bayern warnt davor, Datenschutzbeauftragte ohne hinreichendes Problembewusstsein mit Zusatzaufgaben im Compliance-Bereich zu betrauen.

Ein **Interessenkonflikt des Datenschutzbeauftragten** ergibt sich regelmäßig, wenn dieser im Rahmen seiner sonstigen Tätigkeit für die gleiche Organisation Zwecke und Mittel der Verarbeitung personenbezogener Daten festlegt und sich insofern selbst überwachen müsste. Ob ein Interessenkonflikt i.S.v. Art. 38 Abs. 6 DS-GVO vorliegt, ist nach dem EuGH im Einzelfall auf der Grundlage einer Würdigung aller relevanten Umstände, insbesondere der Organisationsstruktur des Verantwortlichen oder Auftragsverarbeiters, und im Licht aller anwendbaren Rechtsvorschriften, einschließlich etwaiger interner Vorschriften des Verantwortlichen oder des Auftragsverarbeiters, festzustellen.[70]

Inwiefern Zusatzrollen im Hinblick auf die neuen Datenakte zu einer Inkompatibilität hinsichtlich der Tätigkeit als Datenschutzbeauftragter führen, kann also nicht abstrakt, sondern nur unter Berücksichtigung der konkreten Umstände des Einzelfalles beurteilt werden. Entscheidend ist, welche zusätzlichen Aufgaben dem Datenschutzbeauftragten bezüglich der EU-Datenakte konkret zugewiesen werden sollen.

II. Datenschutzbeauftragter und KI-Verordnung: Pflichtaufgaben nach Art. 39 DS-GVO und mögliche Zusatzaufgaben

Insbesondere mit Blick auf die KI-Verordnung ist festzustellen, dass in der Praxis aktuell neue Rollen und Aufgabenzuweisungen entstehen, welche einerseits die Partizipation an dem mit dem KI-Einsatz verbundenen Wertschöpfungspotenzial und andererseits die Beachtung bestehender rechtlicher Anforderungen (Compliance) sicherstellen sollen. Anders als beim Datenschutzbeauftragten, bei dem es sich um eine durch unmittelbar geltendes Recht (Artt. 38 f. DS-GVO) klar definierte Rolle handelt, wird der Inhalt der Rollen bzgl. der KI-Verordnung von den Unternehmen selbst gestaltet und es finden sich in der Praxis nicht nur im Detail unterschiedliche Aufgabenzuweisungen, sondern auch verschiedene Bezeichnungen (insbes. KI-Manager und KI-Beauftragter).

Aufgrund der Vorgaben der DS-GVO dürfen dem Datenschutzbeauftragten keine wesentlichen Entscheidungsbefugnisse in Bezug auf den KI-Einsatz übertragen werden, soweit im Zusammenhang mit der KI personenbezogene Daten verarbeitet werden.

70 EuGH, Urt. v. 09.02.2023 – C-453/21 (X-FAB Dresden), Rn. 45.

Denn würde dem Datenschutzbeauftragten in einem solchen Fall die Verantwortung für den KI-Einsatz übertragen bzw. er diesbezügliche Letztentscheidungen treffen (Prozessfreigabe), so müsste er sich selbst überwachen, was einen Interessenkonflikt i.S.v. Art. 38 Abs. 6 S. 2 DS-GVO begründet.

Wenn auch der Datenschutzbeauftragte nicht über die personenbezogene Datenverarbeitung entscheiden darf, so gehört es doch zu seinem gesetzlichen **Beratungsauftrag (Art. 39 Abs. 1 lit. a) DS-GVO)**, die Entscheidungsfindung durch die Fachverantwortlichen entsprechend zu unterstützen. Zwar bezieht sich dieser Auftrag originär nur auf datenschutzrechtliche Aspekte.

Zeitliche Ressourcen des Stelleninhabers vorausgesetzt, kann der Beratungs- und Überwachungsauftrag auch auf weitere Aspekte bezogen werden, wie etwa die Einhaltung der mit dem KI-Einsatz verbundenen weiteren rechtlichen Rahmenbedingungen neben dem Datenschutz. Hierzu gehören insbesondere die Vorgaben der KI-VO, aber etwa auch die Regelungen des Antidiskriminierungsrechts (AGG) und des Urheberrechts.

Für eine solche Erweiterung der Beratungspflicht spricht jedoch, dass es auf diese Weise nur eine zentrale Anlaufstelle rund um den KI-Einsatz gibt und sich die Fachverantwortlichen nicht mit verschiedenen Ansprechpartnern auseinandersetzen müssen, die ggf. zu unterschiedlichen Wertungen kommen. Letzteres zu vermeiden ist auch deshalb wichtig, weil das Datenschutzrecht eine Querschnittsmaterie ist und sich zwischen dem Datenschutzrecht und den anderen durch die KI betroffenen Rechtsgebieten zum Teil Wechselwirkungen ergeben, so z.B. zwischen AGG und DS-GVO. Um Interessenkonflikte im Hinblick auf die Tätigkeit als Datenschutzbeauftragter zu vermeiden, scheint es allerdings geboten, die Gewährleistungen der **Unabhängigkeit und Weisungsfreiheit** in diesen Fällen durch entsprechende Stellenbeschreibung auch auf die zusätzlichen Beratungsgegenstände zu erstrecken.

Keinen Interessenkonflikt wird es im Übrigen begründen, wenn dem Datenschutzbeauftragten im Zusammenhang mit KI-Projekten **Koordinations- und Dokumentationsaufgaben** übertragen werden. In jedem Fall ist er im Hinblick auf Art. 38 Abs. 1 DS-GVO frühzeitig einzubeziehen in entsprechende Projekte, es sei denn, es werden im Rahmen des konkreten Anwendungsszenarios offenkundig keine personenbezogenen Daten verarbeitet.

Mitglied werden? Mehr Informationen?

https://www.gdd.de/mitglieder/werden-sie-gdd-mitglied/ oder eine E-Mail an: info@gdd.de

Eine Mitgliedschaft bietet wesentliche Vorteile:

>> Mitglieder-Nachrichten mit aktuellen Fachinformationen
>> Bezug der Fachzeitschrift RDV (Recht der Datenverarbeitung)
>> Beratung bei konkreten Einzelfragen
>> Zugriff auf Rechtsprechungs- und Literaturarchiv (in der GDDcommunity)
>> Online-Service „DataAgenda Plus“ (Muster, Checklisten, RDV ONLINE Archiv, Arbeitspapiere etc.)
>> Mitarbeit in Erfahrungsaustausch- und Arbeitskreisen
>> Teilnahme an den kostenfreien GDD-Informationstagen sowie Vergünstigungen bei Seminaren u.v.m.

Schließen Sie sich unseren mehr als 3.600 Mitgliedern an. Eine Mitgliedschaft erhalten Sie schon ab 150,- EUR/Jahr für Privatpersonen und ab 300,- EUR/Jahr für Firmen.

Diese Praxishilfe wurde erstellt durch:

Maximilian Olker
Referent und Doktorand, GDD e.V., Bonn
Clemens Loke
Referent und Doktorand, GDD e.V., Bonn
Henry Simwinga, LL.M. (Göttingen), LL.M. (Liverpool)
Referent, GDD e.V., Bonn
RAin Yvette Reif, LL.M.
GDD e.V., Bonn

Satz: C. Wengenroth, GDD-Geschäftsstelle, Bonn
Stand: Version 2.0 (Juli 2024)

Herausgeber:
Gesellschaft für Datenschutz und Datensicherheit (GDD e.V.)
Heinrich-Böll-Ring 10
53119 Bonn

Tel.: +49 2 28 96 96 75-00
Fax: +49 2 28 96 96 75-25
www.gdd.de
info@gdd.de