Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

# Übersicht über Data Act und weitere EU-Digitalrechtsakte mit Blick auf mögliche Berührungspunkte zum Informationsfreiheitsrecht

Susanne Möhring, BfDI Referat 11
zum TOP **„Data Act und Informationsfreiheitsgesetze“**
bei Arbeitskreis Informationsfreiheit [VK, 8. Mai 2024, 9.00 Uhr]

Liebe Kolleginnen und Kollegen,

## I. [Einleitung]

Ich freue mich über die Gelegenheit, für Sie und mit Ihnen einen Blick in die EU-Digitalrechtsakte, u.a. den DA und den DGA, zu werfen, um eine Übersicht zu gewinnen und die Gesetze und Vorschriften im Verhältnis zueinander und zum geltenden Informationsfreiheitsrecht[1] einordnen zu können.[2]

Manche Regelungen sind erwähnt, weil es möglicherweise parallele oder ähnliche Formulierungen im Informationsfreiheitsrecht gibt und sie als Vorbild dienen oder bei der Auslegung nutzbar sein könnten. Manches habe ich mit aufgenommen, um Ihnen bestimmte Schlüsselworte und Kernregelungen der neuen EU-Gesetze vorzustellen.

Dabei wird der Kreis der Digitalrechtsakte nicht einheitlich verstanden; dieser Überblick betrachtet folgende EU-Verordnungen:

1. DMA (Digital Markets Act)[3]
   Geltung ab 1. November 2022 (Art. 3 Abs. 5,6; Art. 40, 46-50), ab 25. Juni 2023 (Art. 42, 43), ab 2. Mai 2023 (übrige Artikel).

[1] Und auch zum DS-Recht

[2] Eine tabellarische Übersicht bieten auch: Pfeiffer/Helmke, Die Digitalrechtsakte der EU, Teil I – IV, Teile I/II/III in ZD-Aktuell 2023, 1125ff/1162ff/1175ff/

[3] VERORDNUNG (EU) 2022/1925 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 14. September 2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte)

2. DSA (Digital Services Act)[4]
   Geltung ab 16. November 2022 (div. Art./Absätze), ab 17. Februar 2024 (im übrigen).
   Nationale Umsetzung/Ergänzung: Digitale-Dienste-Gesetzvom 6. Mai 2024, BGBl 2024 I Nr. 149, ab 14. Mai 2024 in Kraft.
3. DGA (Digital Governance Act)[5]
   Geltung ab 24. September 2023.
   Die nationale Umsetzung steht noch aus; Referentenentwurf eines Daten-Governance-Gesetzes liegt vor (Stand: Nov. 2023)
4. DA (Data Act)[6]
   Geltung ab 12. September 2025 (weitere geltungsrelevante – später liegende – Daten in Art. 50 DA[7]). Die nationale Umsetzung steht noch aus.

Es können sich darüber hinaus Bezüge ergeben zur ePrivacy-Richtlinie, zur OpenData/PSI-Richtlinie, zur Geschäftsgeheimnis-Richtline, zur P2B-Verordnung u.a.

Als aktuellster Rechtsakt in diesem Zusammenhang soll die KI-VO[8] wenigstens Erwähnung finden – ohne sie näher zu betrachten.

---

[4] VERORDNUNG (EU) 2022/2065 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste)

[5] VERORDNUNG (EU) 2022/868 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 30. Mai 2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (DatenGovernance-Rechtsakt)

[6] VERORDNUNG (EU) 2023/2854 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828 (Datenverordnung)

[7] Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in Kraft. Sie gilt ab dem 12. September 2025. Die Verpflichtung gemäß Artikel 3 Absatz 1 gilt für vernetzte Produkte und die mit ihnen verbundenen Dienste, die nach dem 12. September 2026 in Verkehr gebracht wurden. Kapitel III gilt nur in Bezug auf Datenbereitstellungspflichten nach dem Unionsrecht oder nach im Einklang mit Unionsrecht erlassenen nationalen Rechtsvorschriften, die nach dem 12. September 2025 in Kraft treten. Kapitel IV gilt für Verträge, die nach dem 12. September 2025 geschlossen wurden. Kapitel IV gilt ab dem 12. September 2027 für Verträge, die am oder vor dem 12. September 2025 geschlossen wurden, sofern a) sie unbefristet sind oder b) ihre Geltungsdauer frühestens 10 Jahre nach dem 11. Januar 2024 endet.

[8] KI-VO / AI Act : Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über

Das EU-Digitalrecht bildet eine Querschnittsmaterie auf Grundlage der Digitalstrategie der EU, zu der auch die Datenstrategie der EU (mit DA und DGA) gehört[9]. Es stützt sich meist auf Art. 14 AEUV: Wirtschaftsrecht. Die datenbasierten Geschäftsmodelle haben erhebliche wirtschaftliche Relevanz und nutzen Datenauswertungen zur Steuerung und Bindung der Nutzer und zur Werbung.[10]

## II. Kurzer Blick in den DMA

Als Hinweis vorweg: Schon die Bezeichnung zeigt die wirtschaftliche Bedeutung von Daten und ihrer Nutzung durch Auswertung, die die Grundlage für verschiedene (erfolgreiche) Geschäftsmodelle bildet.

Das **Ziel** des DMA liegt in der Festlegung fairer Geschäftspraktiken zur Schaffung fairer und bestreitbarer Märke im digitalen Sektor.

**Adressiert** werden „Gatekeeper“, das sind Plattformdienste, die von der Kommission nach bestimmten Voraussetzungen benannt werden (*Art. 3 DMA*). Die Liste weist u.a. Alphabet, Amazon, Apple, Meta und Microsoft aus.

Zentrale sich aus dem DMA ergebende **Pflichten** finden sich in *Art. 5 und 6 DMA*; darunter umfangreiche Transparenzpflichten:

Die Gatekeeper/Plattformen müssen Auskunft geben und Daten zur Verfügung stellen, die bei der Nutzung der Plattform generiert werden, z.B. zu Reichweite und Einnahmen aus der platzierten Werbung (*Art. 6 Abs. 10 DMA*). Zudem müssen sie Datenübertragbarkeit gewährleisten (*Art. 6 Abs. 9 DMA*). Besondere Nutzungseinschränkungen gelten für personenbezogene Daten: Die Gatekeeper dürfen Kundendaten nicht für eigene Zwecke verwenden oder zusammenführen (*Art. 5 Abs. 2 b - d DMA*).

Die Umsetzung und Überwachung übernimmt die EU-Kommission, in Deutschland ggf. mit Hilfe des Bundeskartellamts.

## III. Kurzer Blick in den DSA

Der DSA hat zum **Ziel**, das Online-Umfeld sicher, berechenbar und vertrauenswürdig zu machen, damit Bürgerinnen und Bürger ihre Grundrechte – Meinungs- und

---

künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der EU COM (2021) 206 final, vom 21. April 2021; politische Einigung am 9.12.2023

[9] Datenrecht umfasst „nur“ DA und DGA (EU Datenstrategie: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_de); EU-Digitalrechtsakte / EU-Digitalstrategie geht weiter (https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_de).

[10] Apel/Huber, Das neue Datenrecht der EU – Eine Übersicht, Teil 1, JuS 2024 S. 410 ff)

Informationsfreiheit, unternehmerische Freiheit, Verbraucherschutz – ausüben können, was ein verantwortungsvolles Verhalten der Anbieter von Vermittlungsdiensten erfordert (*ErwGrd 3 DSA*).

Die **adressierten** Vermittlungsdienste bieten Durchleitung/Zugang zu einem Kommunikationsnetz oder Caching oder Hosting an und bilden 4 Kategorien:

- VLOP/VLOSE (Very large online platforms / search engines)
- Online-Platform (wie Marktplätze, Appstores, Social Media-Käufe)
- Hosting-Services (mit Cloud- und Web-Hosting) und
- Intermediary Services (Vermittlungsdienste = Internetanbieter)

VLOP/VLOSE werden von der EU-Kommission in einer Liste geführt, die bisher u.a. Amazon, Apple, Booking.com, Google, LinkedIn, Microsoft, Tiktok, Wikimedia, Twitter und Zalando umfasst.

Die **Pflichten** – von denen ich hier nur die zentralen nenne - sind je nach Kategorie differenziert. Vermittlungsdienste unterliegen vor allem einer Transparenzpflicht und müssen über die Moderation von Inhalten und Beschwerden berichten (*Art. 15 DSA*). Hosting-Dienste müssen zusätzlich Melde- und Abhilfeverfahren für rechtswidrige Inhalte einrichten und Straftaten melden. (*Art. 16 – 18 DSA*). Online-Plattformen müssen darüber hinaus vertrauenswürdige Hinweise ermöglichen, interne Beschwerdesysteme einrichten, Informationen über Werbung und über die Empfehlungsalgorithmen geben (*Art. 22, 24, 26, 27 DSA*). Wenn sie Fernabsatzverträge ermöglichen, müssen die Plattformen zudem über die Unternehmer (Verkäufer) informieren können (*Art. 29 ff DSA*).

VLOP/VLOSE gewähren Zugang zu ihren Daten

- dem Koordinator für digitale Dienste zu Überwachungszwecken (*Art. 40 Abs.1 DSA*)
- auf begründetes Verlangen des Koordinators für digitale Dienste: zugelassenen Forschern für Erforschung systemischer Risiken (*Art. 40 Abs. 4, Art. 8 DSA)*

Der DSA lässt andere EU-Vorschriften ausdrücklich unberührt, u.a. die DSGVO (*Art. 2 Abs. 4 lit g) DSA*)

Die nationale Umsetzung im Digitale-Dienste-Gesetz[11] löst das Telemediengesetz ab, errichtet die Koordinierungsstelle für digitale Dienste bei der Bundesnetzagentur (*Art. 49 ff DSA , § 14 DDG*), und legt in § 12 verschiedene Zuständigkeiten fest[12],)

[11] Gesetz zur Durchführung der Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG sowie zur Durchführung der Verordnung (EU) 2019/1150 des Europäischen

## IV. Blick in den DGA

Der DGA hat zum **Ziel**, einen harmonisierten Rahmen für Datenaustausch zur Verbesserung der gemeinsamen Datennutzung im Binnenmarkt zu bieten. Er will für eine vertrauenswürdige und sichere Datengesellschaft und Datenwirtschaft sorgen und soll durch Regelungen zu den geplanten Datenräumen[13] ergänzt werden (*ErwGrd 3 DGA*). Er will auch die die Verwendung und Weiterverwendung von Daten der öffentlichen Stellen stärken und einen Rahmen für Datenaltruismus schaffen (*ErwGrd 5 DGA).*

Dabei bleiben (nationale) Bestimmungen über den Zugang zu oder die Weiterverwendung von Daten unberührt *(Art. 1 Abs. 2 DGA).* Der DGA begründet weder eine Verpflichtung für öffentliche Stellen, die Weiterverwendung von Daten zu erlauben, noch befreit der DGA öffentliche Stellen von bestehenden Geheimhaltungspflichten (*Art. 1 Abs. 2*).

Er **adressiert** Dateninhaber, die – so die Definition – berechtigt sind, zu bestimmten Daten Zugang zu gewähren oder diese weiterzugeben (*Art. 2 Nr. 8 DGA*). Hierzu gehören auch öffentliche Stellen, wie Gebietskörperschaften und öffentliche Einrichtungen, zu denen wiederum juristische Personen zählen, die einen Zweck im allgemeinen Interesse erfüllen und öffentliche finanziert und kontrolliert werden (*Art. 2 Nr. 17, 18 DGA*). Er adressiert auch Datenvermittlungsdienste, die betroffene Personen und Dateninhaber mit Datennutzern mittels Geschäftsbeziehung verbinden (*Art. 2 Nr. 11*, zu unterscheiden von „Vermittlungsdiensten“ nach DSA).

Wesentliche Inhalte und **Pflichten** sind zunächst für <u>öffentliche Stellen</u> festgelegt *(Kapitel II, Art. 3 – 9 DGA)*. Die Regelungen gelten für Daten im Besitz der öffentlichen Stellen, die besonders geschützt sind: Geschäftsgeheimnisse, Statistikgeheimnis, Urheberrechtsschutz und personenbezogene Daten (*Art. 3 Abs. 1 DGA*). Dies sind gerade die Daten, die von der Open-Data/PSI-Richtlinie[14]

---

Parlaments und des Rates vom 20. Juni 2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten und zur Änderung weiterer Gesetze

[12] u.a. für BfDI bzgl. Profiling (Art. 26, 28 DSA)

[13] Beispielweise als erster von 14 Datenräumen: Europäischer Gesundheitsdatenraum (European Health Data Space, EDHS, über den „Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über den europäischen Raum für Gesundheitsdaten COM (2022) 197 final, vom 5. Mai 2022“; soll im Herbst beschlossen werden).

[14] Richtlinie (EU) 2019/1024

ausgenommen sind (*ErwGrd 10 DGA*). Nicht erfasst sind Daten öffentlicher Unternehmen, Rundfunkanstalten, Kultur- und Bildungseinrichtungen, aus Gründen der öffentlichen Sicherheit besonders geschützte Daten und Daten, deren Bereitstellung nicht unter den gesetzlich festgelegten öffentlichen Auftrag[15] fällt.
Die oben genannten geschützten Daten sollen unter besonderen Bedingungen durch Dritte weiterverwendet bzw. genutzt werden können, weil sie mit öffentlichen Geldern generiert wurden *(ErwGrd 6 DGA*). Für diese Nutzung können die öffentlichen Stellen Anforderungen stellen, um zugleich den Schutz der Daten zu gewährleisten. Hierzu zählen u.a.: Anonymisierung, Aufbereitung/Aggregierung, Fernzugriff auf eine gesicherte Verarbeitungsumgebung (*Art. 5 Abs. 3 DGA*), ggf. muss die Nutzende Partei vertraglich Geheimnisschutz zusichern (*zB Art. 5 Abs. 10 DGA*). Zu Mustervereinbarungen und Drittstaatenregelungen kann es noch Durchführungsrechtsakte geben.
Dabei ist zu berücksichtigen, dass die DSGVO unberührt bleibt, im Konfliktfall vorgeht und die Regelungen des DGA keine eigene Verarbeitungsgrundlage darstellen *(Art. 1 Abs. 3 / ErwGrd 4 DGA*). Hier dürften offene Fragen und Abgrenzungsschwierigkeiten verbleiben.
Für die Nutzung dürfen die öffentlichen Stellen Gebühren erheben (*Art. 6 DGA*).
Deutschland hat die zuständige Stelle nach Art. 7 DGA noch nicht benannt (Stand 15.4.2024), gute Aussichten dürfte die Bundesnetzagentur haben.
Weitere **Inhalte**:
Kapitel III enthält Maßgaben für Datenvermittlungsdienste – teilweise auch als Treuhandstellen oder Datentreuhandplattform bekannt – u.a. die Voraussetzungen für die Anmeldung und Anerkennung. Ein entsprechendes Logo gibt es schon („EU Recognised Data Intermediary“). Der Tätigkeitsinhalt ist in Art. 12 DGA beschrieben.
Zudem werden die Bedingungen für Datenaltruistische Organisationen geregelt, die auf Grundlage von Einwilligungen der betroffenen Personen bzw. mit Erlaubnis der Dateninhaber die Nutzung der Daten durch Dritte für Ziele von allgemeinem Interesse ermöglichen (*Art. 2 Nr. 16, Art. 16 ff DGA*). Sie werden anerkannt und in ein Register eingetragen. Es gibt ein Logo: „EU Recognised Data Altruism Organisation“ (RDAO). Das einheitliche Einwilligungsformular wird vom European

[15] Parallele Formulierung (aber Dokument statt Daten): Art. 1 PSI RL

Data Innovation Board (EDIB; Dateninnovationsrat, *Art. 29 DGA*) entwickelt (*Art. 25 DGA*).

## V. Blick in den DA

**Ziel** des Data Act ist das Schaffen eines harmonisierten Rahmens mit Bedingungen und Grundlagen für die Nutzung und den Zugriff auf Daten von Produkten oder verbundenen Diensten (*ErwGrd 4 DA*). Wesentlicher Anwendungsbereich sind beispielsweise Geräte im Internet of Things (IoT) und Daten aus Fahrzeugen sowohl im Verhältnis zum Verbraucher (B2C) als auch im Verhältnis zwischen Unternehmen (B2B).

Der Data Act **adressiert** dementsprechend vor allem Produkthersteller, aber auch Dateninhaber (*Art. 2 Nr. 6 DA*) und öffentliche Stellen (*Art. 2 Nr. 9 DA*). Zu beachten ist: Die Definitionen weichen etwas von denen im DGA ab. Und: die öffentlichen Stellen sind fast ausschließlich in der Rolle als Datenempfänger gemeint. Allerdings können öffentliche Unternehmen durchaus als Dateninhaber fungieren (*ErwGrd 63 S. 3 DA*)

Zu den wesentlichen **Pflichten** zählt die „accessibility / data access by design“, also die Konzipierung von Produkten und vernetzten Diensten so, dass deren Daten – einschließlich der Metadaten – standardmäßig für den Nutzer einfach, sicher unentgeltlich in einem umfassenden, strukturierten, gängigen und maschinenlesbaren Format und – soweit möglich – direkt zugänglich sind (*Art. 3 Abs. 1 DA*). Falls kein direkter Datenzugriff möglich ist, stellt der Dateninhaber die Daten dem Nutzer unverzüglich[16] zur Verfügung (*Art. 4 Abs. 1 DA*). Aufgrund dieser zentralen Anspruchsnorm haben die Nutzer das Recht auf Zugang zu den von ihnen erzeugten Daten. Entsprechend gibt es Informationspflichten bezüglich der durch das Produkt oder den Dienst generierten Daten (in Art. 3 Abs. 2 und 3 DA).

Beschränkungen des Zugangs und der Weiterverwendung sind auf vertraglicher Grundlage möglich, wenn dadurch Sicherheitsanforderungen beeinträchtigt werden (*Art. 4 Abs. 2 DA*). Zur Wahrung von Geschäftsgeheimnissen vor allem gegenüber Dritten müssen besondere Maßnahmen getroffen werden, ein Ausschluss der Auskunft kommt nur ausnahmsweise in Betracht. (*Art. 4 Abs. 6 DA*).

[16] Einschließlich der Metadaten unverzüglich, einfach, sicher, unentgeltlich, in einem umfassenden, gängigen und maschinenlesbaren Formal und – soweit möglich- in der gleichen Qualität kontinuierlich und in Echtzeit bereit..
Auf einfaches elektronisches Verlangen

Auf Verlangen des Nutzers muss der Dateninhaber Daten auch an Dritte zur Verfügung stellen (*Art. 5 DA*). Bei der Datenbereitstellung sind die FRAND-Bedingungen einzuhalten (fair, reasonable, non-discriminatory; fair, angemessen, nichtdiskriminierend, *Art. 8 DA*). Das Diskriminierungs- und Exklusivitätsverbot gilt auch für technische Schutzmaßnahmen, die niemanden ausschließen dürfen (*Art. 11 DA*). Für Dritte als Datenempfänger geltende verschiedene Verbote, u.a. Untersagung der zweckwidrigen Verwendung, der Weitergabe, des Verstoßes gegen vereinbarte Bedingungen (*Art. 6 DA*).

Weitere **Inhalte**:

Kapitel V regelt die Voraussetzungen und Bedingungen, nach denen eine öffentliche Stelle von einem Dateninhaber Datenbereitstellung verlangen kann. Dies setzt eine außergewöhnliche Notwendigkeit für die Erfüllung der Aufgabe im öffentlichen Interesse voraus (*Art. 14 ff. DA*). Diese Verpflichtung zur Bereitstellung dieser Daten gilt nicht für öffentliche Stellen (*Art. 14 a.E.*). Verlangt eine öffentliche Stelle unter dem DA die Bereitstellung von Daten, ist das Datenverlangen zu veröffentlichen (*ErwG 69, Art. 17 Abs. 2 lit. g DA*).

Kapitel VII regelt im Hinblick auf die geplanten Datenräume besondere Anforderungen an die Interoperabilität (Art. 33 ff DA) sowie Vorgaben für sog. intelligente[17] Verträge (*Art. 36 DA*).

Bei der nationalen Umsetzung, die noch aussteht, hat die BNetzA gute Chancen als zuständige Behörde (*Art. 37 DA*) benannt zu werden.

## VI. Fazit

- DMA und DSA sind aus informationsfreiheitlicher Perspektive wenig relevant, zumal öffentliche Stellen nicht adressiert sind.
- Der DGA ergänzt das Informationsfreiheitsrecht quasi komplementär; lässt die Informationsfreiheit unberührt und begründet für öffentliche Stellen unmittelbar weder Zugangsrechte noch. Veröffentlichungspflichten
- Der DA weist wenig Überschneidungen zur Informationsfreiheit auf und führt öffentliche Stellen (nur) als Datenempfänger

Es ist vieles noch offen und es wird in der konkreten Anwendung eine Fülle von Auslegungs- und Abgrenzungsproblemen geben

[17] Definition in Art. 2 Nr. 39: Ein Computerprogramm, das für die automatisierte Ausführung einer Vereinbarung … verwendet wird, wobei eine Abfolge elektronischer Datensätze verwendet wird … ~~ deren Integrität und chronologische Reihenfolge gewährleistet werden.