

Everything, everywhere all at once – Neue Konzepte der Daten- regulierung in der EU

Briefing

Neue Konzepte der Datenregulierung in der EU



Daten sind heutzutage die entscheidende Grundlage für Innovationen, wirtschaftliches Wachstum und technologische Entwicklungen. Ähnlich wie Öl in der Industrialisierung treiben Daten alle Bereiche der modernen Wirtschaft an – von künstlicher Intelligenz über personalisierte Dienstleistungen und Werbung bis hin zu Smart Cities. Unternehmen und staatliche Institutionen nutzen Daten, um bessere Entscheidungen zu treffen, Prozesse zu optimieren und neue Produkte zu entwickeln. Ein Blick in die Zukunft verrät, dass der Wert von Daten mit der wachsenden Vernetzung und Digitalisierung weiterhin exponentiell steigen wird.

Auch die EU hat diese Entwicklung erkannt und setzt das bislang ungenutzte Potenzial der europäischen Datenunion an die höchste Stelle ihrer politischen Tagesordnung. Ihr Ziel ist es, einen „vereinfachten, klaren und kohärenten Rechtsrahmen“ zu schaffen, in dem Unternehmen und staatliche Institutionen „nahtlos und in großem Maßstab“ Daten austauschen und verwenden können.¹ Dabei verfolgt sie einen holistischen Ansatz: Nicht nur soll der Umgang mit Daten neu definiert werden. Auch sollen datengetriebene Märkte fair und bestreitbar gestaltet und die Marktmacht großer Digitalkonzerne beschränkt werden. Gleichzeitig sollen die (Grund-)Rechte und Freiheiten der Bürger sowie zentrale europäische Werte gewahrt bleiben.²

Damit verfolgt die EU ein auf den ersten Blick widersprüchliches Ziel, durch zusätzliche Regulierung bisher bestehende Schranken für den Austausch von Daten abzubauen und einen florierenden europäischen Binnenmarkt für Daten zu schaffen. Wie sich aber etwa aus dem im September 2024 veröffentlichten Bericht des ehemaligen EZB-Präsidenten und ehemaligen italienischen Ministerpräsidenten Mario Draghi zur Zu-

kunft der Wettbewerbsfähigkeit der EU ergibt, steht dahinter ein nachvollziehbarer Befund. Bis dato leidet eben jener Binnenmarkt nämlich nicht zuletzt daran, dass Unternehmen aufgrund unterschiedlicher mitgliedsstaatlicher Gesetze bzw. fragmentierter Durchsetzung von EU-Regulierung hohe Compliance-Kosten haben.³

Die EU steht somit vor der Herausforderung, den regulatorischen Spagat zu meistern, die branchenübergreifende Nutzung von Daten sowie die Innovationsfähigkeit und den Wettbewerb zu fördern, gleichzeitig aber auch die europäischen Werte zu wahren. Eine maßgebliche Rolle hierbei wird die neue exekutive Vizepräsidentin der Europäischen Kommission für Technische Souveränität, Sicherheit und Demokratie Henna Virkkunen spielen. Ihr wurde von der Präsidentin der Europäischen Kommission, Ursula von der Leyen, in einem „Mission Letter“ unter anderem auferlegt, eine Strategie für eine europäische Datenunion vorzulegen.⁴

Im Spannungsfeld all dieser Faktoren nimmt das europäische Datenrecht bereits Schritt für Schritt Konturen an.

I. Welche Ziele verfolgt die EU im Rahmen ihrer Datenregulierung?

Die EU strebt danach, eine der attraktivsten, sichersten und dynamischsten Datenwirtschaften weltweit zu werden. Dabei ist sich die Kommission der Komplexität des digitalen Raums bewusst, in dem zahlreiche Interessen, Risiken und Chancen in Bezug auf die Nutzung von Daten ausbalanciert werden müssen. Fünf Leitziele sollen helfen, einen sicheren, fairen und zukunftsfähigen digitalen Raum in der EU zu etablieren:

¹ Vgl. Europäische Kommission, Mitteilung vom 19.02.2020, COM(2020) 66 final, insb. S. 1 <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52020DC0066>, abgerufen am 18.12.2024.

² Vgl. Europäische Kommission, Mitteilung vom 19.02.2020, COM(2020) 66 final, insb. S. 9, 27 f., <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52020DC0066>, abgerufen am 18.12.2024.

³ Vgl. Europäische Kommission, The future of European Competitiveness Part A, S. 30, https://commission.europa.eu/topics/strengthening-european-competitiveness/eu-competitiveness-looking-ahead_en, abgerufen am 18.12.2024.

⁴ Vgl. Europäische Kommission, Mission Letter an Henna Virkkunen vom 17.09.2024, https://commission.europa.eu/document/3b537594-9264-4249-a912-5b102b7b49a3_en, abgerufen am 18.12.2024.

– Schaffung eines europäischen Binnenmarktes für Daten:

Die EU will den freien und sicheren Austausch von Daten innerhalb Europas fördern und damit einen europäischen Binnenmarkt für Daten schaffen. Daten als wichtige Ressource für Innovationen und wirtschaftliches Wachstum sollen zugänglich gemacht und von Bürgern, Unternehmen, Regierungen und Forschungseinrichtungen über Sektoren und Länder hinweg geteilt werden können.

– Eröffnung neuer datengetriebener Märkte:

Die Datenregulierung zielt dabei nicht nur darauf ab, Märkte zum Austausch von Daten als solche zu schaffen. Vielmehr sollen auch neue datengetriebene Märkte entstehen, deren typische Leistung erst durch die Verfügbarkeit von Daten möglich wird. Das können insbesondere Märkte sein, auf denen bereits existierende Produkte/Dienstleistungen durch die Auswertung und Nutzung von Daten verbessert werden oder sogar gänzlich neue Produkte/Dienstleistungen angeboten werden.

– Innovation und Wettbewerb fördern:

In diesem Zusammenhang soll auch ein dynamisches digitales Umfeld geschaffen werden, in dem neue Ideen und Technologien gedeihen können, während gleichzeitig ein fairer und offener Wettbewerb gewährleistet wird. Sowohl existierende als auch neu entstehende, datengetriebene Märkte sollen nicht weiter von wenigen Digitalkonzernen dauerhaft dominiert werden, sondern fair und bestreitbar bleiben.

– Datensouveränität stärken:

Neben diesen primär wirtschaftlichen Aspekten will die EU zugleich einen verantwortungsvollen Umgang mit Daten in Übereinstimmung mit europäischen Werten wie Datenschutz und -sicherheit sowie Transparenz sicherstellen.

– Vertrauenswürdigkeit von Technologien gewährleisten:

Hierzu gehört auch die Förderung sicherer, transparenter und zuverlässiger digitaler Systeme, die insbesondere den Schutz von Daten, die Privatsphäre der Nutzer und die Integrität der digitalen Kommunikation gewährleisten.

II. Neue Konzepte der Datenregulierung

Die rechtliche Verankerung dieser Leitziele ist von zentraler Bedeutung für eine kohärente und nachhaltige europäische Datenpolitik. Die EU zeigt dabei klare Handlungsbereitschaft. So hat sie mit der Datenschutz-Grundverordnung (DS-GVO)⁵ bereits einen umfassenden Rechtsrahmen für den Schutz personenbezogener Daten geschaffen. Angesichts der rasanten Entwicklungen im digitalen Bereich hat die EU jedoch auch erkannt, dass weitere regulatorische Anpassungen notwendig sind, um mit der zunehmenden Komplexität des „Datenuniversums“ Schritt zu halten und im globalen Wettbewerb – insbesondere mit den USA und China – nicht abgehängt zu werden. Dem versucht sie durch ihre neuen Konzepte zur Datenregulierung gerecht zu werden.

Während die bisherige Datenregulierung vor allem auf Datenschutz und -sicherheit ausgerichtet war, stößt die EU mit den jüngst ergangenen Rechtsakten in die entgegengesetzte Richtung vor. Eine Vielzahl dieser Rechtsakte regelt die kommerzielle Nutzbarkeit von Daten. Zu nennen sind in diesem Zusammenhang insbesondere der im Rahmen der europäischen Datenstrategie verabschiedete *Data Act*⁶ sowie der *Data Governance Act (DGA)*⁷, die beide die Verfügbarkeit von Daten im europäischen Raum fördern sollen. Hinzu kommen der *Digital Markets Act (DMA)* und der *AI Act*⁸ – beides wegweisende Verordnungen, die zwar nicht primär auf die Datenregulierung abzielen, jedoch erheblichen Einfluss auf die europäische Wirtschaft im digitalen Raum ausüben.

⁵ Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.

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.

⁷ 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.

⁸ Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828.

1. Data Act

Der Data Act zielt darauf ab, den Zugang zu und die Nutzung von Daten – vor allem solcher, die bei der Verwendung vernetzter Produkte erzeugt werden – zu verbessern. Es sollen die für die bislang unzureichende Nutzung der Daten verantwortlichen rechtlichen, wirtschaftlichen und technischen Hindernisse beseitigt und somit eine stärkere Datennutzung in der EU gefördert werden. Der Data Act dient damit nicht zuletzt dem Ziel eines europäischen Binnenmarkts für Daten wie auch der Eröffnung neuer datengetriebener Märkte. Konkret schafft der Data Act neue Datenzugangsrechte und regelt rechtlich zulässige Formen der Datennutzung im B2B- sowie B2C-Bereich, aber auch zwischen Privaten.

Im Mittelpunkt steht dabei die Datenhoheit des Nutzers. So besteht ein sektorübergreifender Zugangsanspruch für Nutzer zu Daten, die von ihren IoT-Produkten und damit verbundenen Diensten generiert werden. Gleichzeitig dürfen Nutzer die Weitergabe dieser Daten durch die Anbieter von IoT-Produkten bzw. von produktbezogenen digitalen Diensten (sogenannte verbundene Dienste) als Dateninhaber im B2B-Verhältnis an Dritte zu fairen, angemessenen und nicht-diskriminierenden Konditionen verlangen. Hierdurch soll es den Dritten etwa ermöglicht werden, auf Grundlage der Daten ergänzende Dienstleistungen und/oder Produkte zu entwickeln. Begrenzt wird dieser Datenzugangsanspruch u. a. durch allgemeine kartellrechtliche Regeln zum unerlaubten Informationsaustausch und Regelungen zu Geschäftsgeheimnissen. Zudem werden die nach dem Digital Markets Act als sogenannte Gatekeeper benannten großen Digitalkonzerne weitgehend vom Datenzugang nach dem Data Act ausgeschlossen.

Vervollständigt wird das Konzept der Datenhoheit durch ein Zustimmungserfordernis: Dateninhaber dürfen künftig von IoT-Produkten generierte Daten nur noch mit vertraglicher Zustimmung des Nutzers nutzen und verwerten. Dies betrifft insbesondere Hersteller von vernetzten Produkten, Anbieter von verbundenen Diensten sowie Datenverarbeitungsdiensten (z. B. Cloud-Computing-Diensten). Darüber hinaus enthält der Data Act Regelungen zu Produkt-Designpflichten sowie AGB-Miss-

brauchskontrollen in Datennutzungsverträgen und zur Interoperabilität von Datenräumen und Datendiensten.

Bei Nichteinhaltung der genannten Pflichten drohen hohe Sanktionen. So können je nach Art, Schwere, Umfang und Dauer des Verstoßes Bußgelder von bis zu EUR 20 Mio. bzw. bis zu 4 % des weltweit erzielten Umsatzes verhängt werden. Dabei können auch frühere Verstöße und durch den Verstoß bedingte finanzielle Gewinne eine Rolle spielen.

Der Data Act ist am 11.01.2024 in Kraft getreten. Anwendung finden wird der Data Act in großen Teilen jedoch erst ab dem 12.09.2025.⁹ Betroffene Unternehmen haben insoweit noch Zeit, ihre Systeme darauf einzustellen.

2. Data Governance Act

Der DGA schafft hingegen einen Rechtsrahmen für die gemeinsame Nutzung von Daten, indem er einen neutralen Zugang zu Daten sowie die Interoperabilität sichern und zur Vermeidung von Lock-in-Effekten beitragen soll.

Dabei zielt der DGA insbesondere auf öffentliche Stellen ab. So sieht er Rahmenbedingungen für die (sicherere) Weitergabe und Wiederverwendung geschützter Daten öffentlicher Stellen vor, die u. a. ein Verbot von Ausschließlichkeitsvereinbarungen für Daten im Besitz öffentlicher Stellen sowie weitere Pflichten zur Ausgestaltung von Datenlizenzenverträgen zwischen öffentlichen Stellen und Privaten beinhalten.

Darüber hinaus regelt der DGA die Datennutzung und -weitergabe durch sogenannte Datenvermittlungsdienste sowie altruistische Organisationen, denen in der heutigen Datenwirtschaft jedoch bislang noch kaum Relevanz zukommt.

Verstöße gegen den DGA können ebenfalls Sanktionen nach sich ziehen. Deren Art ist jedoch von den EU-Mitgliedsstaaten festzulegen. Die für die Einhaltung des DGA national zuständige Behörde ist jedenfalls befugt,

⁹ vgl. Art. 50 S. 2 Data Act.

z. B. Geldbußen zu verhängen oder die Erbringung des Datenvermittlungsdienstes auszusetzen.

3. Digital Markets Act

Der DMA¹⁰ zielt auf die Begrenzung der Marktmacht großer Digitalkonzerne und die Gewährleistung fairer und bestreitbarer Märkte ab. Häufig als „kartellrechtsnahe Regulierung“¹¹ bezeichnet, sind in den Digital Markets Act im Wesentlichen die Erfahrungen der EU bei der kartellrechtlichen Verfolgung eben jener Digitalkonzerne (nicht zuletzt im Zusammenhang mit deren datengetriebenen Geschäftsmodellen) in den letzten Jahren und Jahrzehnten eingeflossen.

Kern des DMA sind umfangreiche Verhaltenspflichten, die für Unternehmen gelten, die vorher von der Europäischen Kommission als Gatekeeper benannt wurden. Die Benennung als Gatekeeper hängt von der Erfüllung bestimmter qualitativer Kriterien durch die von den Unternehmen betriebenen sogenannten zentralen Plattformdienste ab. Diese Kriterien beziehen sich auf den Einfluss und die Bedeutung der Dienste auf digitalen Märkten innerhalb der EU und deren Beständigkeit. Bei Überschreiten bestimmter Schwellenwerte (bzgl. Umsatz/Marktkapitalisierung sowie der Anzahl von gewerblichen Nutzern und Endnutzern) besteht eine starke Vermutung für die Stellung als Gatekeeper. So benannt wurden bisher die Unternehmen Alphabet, Amazon, Apple, Booking, ByteDance, Meta und Microsoft.

Einmal als Gatekeeper benannt, müssen die Unternehmen einen ausführlichen Pflichtenkatalog erfüllen, der in Zukunft durch die Europäische Kommission noch erweitert werden kann. Teil des Katalogs ist dabei auch eine Reihe von datenbezogenen Pflichten und Verboten. So gelten etwa Verbote der Zusammenführung von Daten aus verschiedenen Diensten ohne Einwilligung von Endnutzern, Verbote der Nutzung von Daten im Wettbewerb mit gewerblichen Nutzern und auch verschiedene Datenzugangsansprüche zugunsten von Nutzern der zentralen Plattformdienste. Insgesamt geht es der EU beim DMA im Zusammenhang mit Daten darum, den Wettbewerbsvorsprung der großen Digitalkonzerne auf datengetriebenen

Märkten zu begrenzen und diese Märkte auch für andere Unternehmen zu öffnen (und damit „bestreitbar“ zu machen).

Verstöße gegen den DMA können ebenfalls mit empfindlichen Geldbußen von bis zu 10 % des weltweiten Jahresumsatzes geahndet werden. Im Falle der systematischen Missachtung sieht der Digital Markets Act sogar die Möglichkeit zur Anordnung struktureller Maßnahmen gegenüber den Gatekeepers vor. Zudem soll es der DMA auch den betroffenen Nutzern möglich machen, im Wege des Private Enforcement die Verhaltenspflichten gerichtlich durchzusetzen (z. B. durch Klage auf Datenzugang).

4. AI Act

Der AI Act reguliert zwar nicht originär die Datenverarbeitung. Allerdings ergeben sich auch bei der Verwendung von KI mögliche systemische Gefährdungen von Grundfreiheiten und dem Schutz personenbezogener Daten, denen die EU mit dieser Verordnung begegnen will.

Es handelt sich insoweit um ein präventives, sektorübergreifendes Verbotsgesetz, das den Einsatz von KI in zahlreichen Anwendungsszenarien verbietet oder von technischen, organisatorischen und rechtlichen Anforderungen abhängig macht. So sind bestimmte KI-Systeme, die sensible personenbezogene Daten verarbeiten, per se verboten. Dies betrifft beispielsweise Social-Scoring-Systeme, Profiling in der Strafverfolgung sowie Datenbank-KI-Systeme zur Gesichtserkennung.

Bei der Verwendung anderer KI-Systeme unterliegen Anbieter und Betreiber hingegen zahlreichen Pflichten, die sich nach der jeweiligen Art des KI-Systems richten. Beispielsweise müssen Anbieter bei der Verwendung eines KI-Systems gegenüber natürlichen Personen darauf hinweisen, dass mit einem KI-System interagiert wird. Betreiber eines KI-Systems, das Bild-, Ton- oder Videoinhalte erzeugt oder manipuliert (Deepfake), müssen hingegen offenlegen, dass die Inhalte künstlich erzeugt oder manipuliert wurden.

¹⁰ 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).

¹¹ Vgl. Europäische Kommission, Pressemitteilung vom 15.12.2020, https://ec.europa.eu/commission/presscorner/detail/de/ip_20_2347, abgerufen am 18.12.2024.

Bei Verstößen wegen Missachtung des Verbots bestimmter KI-Praktiken drohen Bußgelder von bis zu EUR 35 Mio. bzw. bis zu 7 % des weltweiten Jahresumsatzes. Im Falle von KI-Modellen mit allgemeinem Verwendungszweck drohen dagegen Geldbußen von bis zu EUR 15 Mio. bzw. 3 % des weltweiten Jahresumsatzes.

III. Was bedeutet das für Unternehmen?

Die neue europäische Regulierung von Daten und KI stellt Unternehmen vor komplexe Aufgaben. Sie stehen vor der Herausforderung, ihre Geschäftsmodelle nicht nur technologischen Entwicklungen anzupassen. Sie müssen sich auch in einem zunehmend komplexen und dichten Netz von regulatorischen Anforderungen orientieren und sicherstellen, dass sie die umfangreichen Compliance-Vorgaben erfüllen. Es geht darum, die Auswirkungen der neuen Regelungen auf das eigene Unternehmen nachzuvollziehen und bestehende Compliance- und Governance-Strukturen soweit erforderlich an die neuen datenzentrierten Regelwerke der EU effizient anzupassen – und zwar schnittstellen- und rechtsgebietsübergreifend.

Dabei steigen die Organisationspflichten und Haftungsrisiken des Managements. Die neuen Regelwerke enthalten eine große Vielzahl neuer und vielschichtiger Pflichten, die sich zum Teil mit anderen Gesetzen überschneiden und in Einzelfällen sich widersprechende Anforderungen enthalten können. Besonders hoch ist die Datenregulierungsdichte in regulierten Industrien wie Banken und Versicherungen, Gesundheit oder Telekommunikation.

Kommt es zu Verstößen gegen die neuen Regulierungen, besteht für das Unternehmen das Risiko immer höher ausfallender Geldbußen und erheblicher Reputationsschäden. Daneben zeigen die Erfahrungen aus dem Datenschutzrecht und dem Kartellrecht, dass das sogenannte Private Enforcement, also (massenhafte) Klagen von Kunden, Verbraucherschutzbehörden oder Wettbewerbern, auch in der EU immer mehr an praktischer Bedeutung gewinnt.

Neben den Compliance-Anforderungen und ihren Auswirkungen auf Produkte und kommerzielle Projekte gilt es auch, ein strategisches Element zu berücksichtigen: Die sogenannte ganzheitliche Datenstrategie. Dabei geht es zum einen um die Frage, wie das Unternehmen seine Daten im Sinne der strategischen Geschäftsziele möglichst gewinnbringend einsetzen kann, und zum anderen, ob die neuen EU-Regelungen ggf. Anknüpfungspunkte bieten, Daten anderer Unternehmen einzuholen und einzusetzen. Die neuen gesetzlichen Anforderungen an die Compliance- und Governance-Strukturen eines Unternehmens hängen ganz wesentlich von den Ausprägungen der Datenstrategie ab.

Dabei gilt es, keine Zeit zu verlieren. Die Pflichten treten gestuft ab 2025 in Kraft. Angesichts der Komplexität der Gesetzesänderungen und des potenziellen Aufwands für die Umsetzung ist es daher höchste Zeit, bestehende Compliance-Strukturen frühzeitig zu evaluieren, um sich auf die neuen gesetzlichen Vorgaben einzustellen und Produkte, Dienstleistungen und Geschäftsprozesse rechtzeitig entsprechend anzupassen. Dieser Prozess sollte nicht als lästige Pflicht, sondern als Chance begriffen werden. Eine klug ausbalancierte Datenstrategie schützt nicht nur vor Haltung und Reputationsverlust. Vor allem ist sie die Basis für künftigen geschäftlichen Erfolg. Unsere Beraterinnen und Berater haben beide Aspekte im Blick und sind darauf spezialisiert, Unternehmen sicher durch die europäische Datenregulierung zu navigieren.

Autorinnen und Autoren



Sarah Blazek

Rechtsanwältin, Partnerin
Brienner Straße 28, 80333 München
sarah.blazek@noerr.com
T +49 89 28628121



Pascal Schumacher

Rechtsanwalt, Partner
Charlottenstraße 57, 10117 Berlin
pascal.schumacher@noerr.com
T +49 30 20942030