Ausgabe 1/2026

BvD-NEWS

Fachmagazin für Datenschutzbeauftragte

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

mastodon.social/@bvd@privacyofficers.social

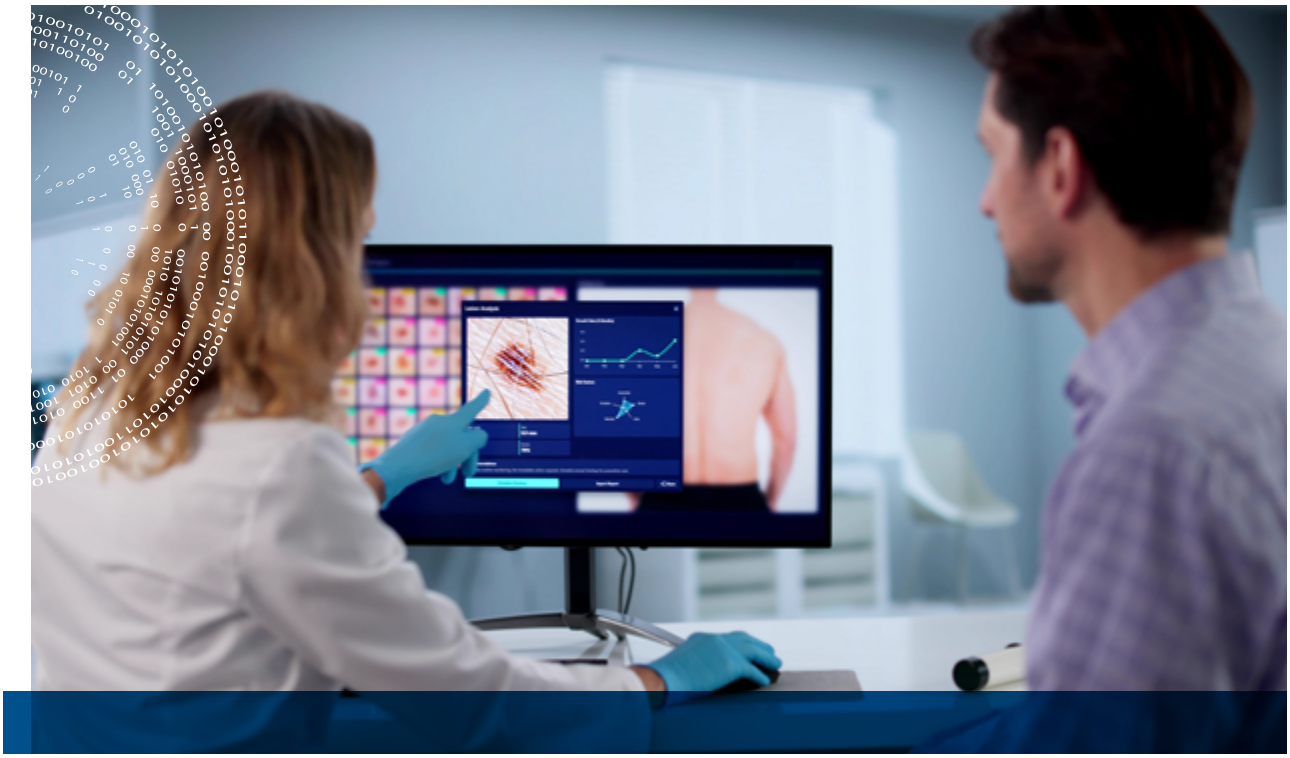
linkedin.com/company/berufsverband-der-datenschutzbeauftragten

BvD e.V.
DATENSCHUTZ GESTALTEN

KRISTINA SCHREIBER

DIE EU-DATENSTRATEGIE UND DER DATA ACT

Weichenstellung für die Datenwirtschaft, mit oder ohne Datenschutz?



Die Datenstrategie der Europäischen Union (EU) ist Teil der EU-Digitalisierungsstrategie, die den digitalen Wandel, die digitale Transformation begleitet und befördert. Im Zentrum der EU-Datenstrategie steht die Verordnung (EU) 2023/2854, als Data Act bezeichnet. Der Data Act ist seit Januar 2024 in Kraft und seit September 2025 anwendbar. Das Ziel der EU-Datenstrategie: Die bestmögliche Nutzung von Daten als Rohstoff, Wettbewerbsfaktor und Innovationstreiber sicherzustellen und dabei die Rahmenbedingungen auf allen Ebenen, technisch wie rechtlich, zu harmonisieren.

Dieses Zielbild scheint in diametralem Widerspruch zum Telos des Datenschutzrechts zu stehen, das mit dem Verbotsprinzip und der Datenminimierung die Datennutzung jedenfalls prima facie tendenziell eindämmen will.

Der vorliegende Artikel geht der Frage nach, welche Auswirkungen der Data Act auf die Datennutzung haben wird – und wie sich dies mit dem Datenschutzrecht vereinbaren lässt.

Paradigmenwechsel: Vom Datensilo zur geteilten Ressource

Das Hauptdefizit der EU-Datenwirtschaft war bislang nicht ein Mangel an Daten, sondern ein Mangel an Datennutzung. Zu viel wertvolles Wissen bleibt in Silos oder hinter rechtlichen Unsicherheiten verborgen, Daten werden nicht in ausreichendem Maße genutzt[1], Potenziale für Innovation, Wettbewerbsfähigkeit und Nachhaltigkeit wurden verschenkt. Umfragen zufolge sind maßgebliche Gründe dafür die Rechtsunsicherheit beim Datenteilen sowie eine fehlende Kompatibilität von Daten.[2]

Der Data Act setzt genau an diesen Defiziten der Datennutzung an. Ziel ist eine gerechtere Verteilung der Datenwertschöpfung und eine erhöhte Verfügbarkeit von Daten zur Entwicklung neuer Geschäftsmodelle. Über die Verwertung der Daten soll dabei der Nutzer entscheiden, da es die entsprechenden Daten ohne seine Produktnutzung nicht gäbe. Um hier einen fairen Austausch abzusichern, dürfen einer-

[1] EU-Kommission, Datenstrategie, 19.02.2020, COM (2020) 66 final, S. 8 f.

[2] Bitkom, Data Economy Studienbericht 2025, S. 15, abrufbar unter https://www.bitkom.org/sites/main/files/2025-09/bitkom-studienbericht-data-economy.pdf (zuletzt abgerufen am 28.02.2026)

seits die großen digitalen Akteure keine Datenempfänger sein (z.B. Google oder Meta), andererseits sind die Datenempfänger gehindert, die erhaltenen Daten im Wettbewerb zum Dateninhaber zum eigenen Vorteil zu nutzen.

Der Data Act soll so zum Motor der Datenwirtschaft werden – und lässt die DSGVO „unbeschadet". Dieser Befund ist ernüchternd: Trotz der weitreichenden Auswirkungen und dem offensichtlich drohenden Zielkonflikt enthält sich der Data Act einer eindeutigen Abgrenzung zum Datenschutzrecht und einer systematischen Verzahnung mit diesem. Der Data Act überlässt dies letztlich der Anwendungspraxis und produziert damit neue Rechtsunsicherheit. Denn obwohl der Data Act auch die Verarbeitung personenbezogener Daten erfasst und etwa auch ein Zugangsrecht zu diesem vorsieht, heißt es in Art. 1 Abs. 5 Satz 1 Data Act lediglich: „Diese Verordnung gilt unbeschadet des Unionsrechts und des nationalen Rechts über den Schutz personenbezogener Daten …, insbesondere der Verordnungen (EU) 2016/679 und (EU) 2018/1725 und der Richtlinie 2002/58/EG, einschließlich der Befugnisse und Zuständigkeiten der Aufsichtsbehörden und der Rechte der betroffenen Personen."

Systematik des Data Act mit sektorübergreifenden Leitplanken

Der Data Act umfasst eine Reihe von nebeneinander stehenden Verpflichtungen, insbesondere die Pflicht zur Gewährung eines Datenzugangs in Echtzeit, die Ermöglichung eines einfachen Wechsels von Datenverarbeitungsdiensten (sog. Cloud-Switching), das Gebot fairer Vertragsklauseln zur Datenverwendung und eine Bereitstellungspflicht im Fall öffentlicher Notstände oder außergewöhnlicher Bedürfnisse der öffentlichen Hand. In einen Konflikt mit dem Datenschutzrecht kann insbesondere der erste Block geraten, das Datenzugangsrecht.

Mit den Regelungen zum Datenzugang sieht der Data Act Verpflichtungen zur Bereitstellung von und zum Zugang zu Daten vor, die bei der Nutzung von vernetzten Produkten und verbundenen Diensten („smart products", IoT) entstehen. Nutzungs- und Produktdaten, ob personenbezogen oder nicht, werden für Nutzer – Unternehmen und Verbraucher – zugänglich, und zwar ab September 2026 „by default" und „by design". Bis dahin müssen die Daten bereitgestellt werden, möglichst ohne Hürden und in Echtzeit. Für die Praxis heißt das: Hersteller und Diensteanbieter müssen ab diesem Jahr Produkte und verbundene Dienste so konzipieren, dass ein leicht nutzbarer, maschinenlesbarer, sicherer Datenzugang geschaffen wird. Ein direkter Zugang durch Schnittstellen ist das Ziel. Gelingt dies nicht, greift die gesetzliche Datenbereitstellungspflicht durch den jeweiligen Dateninhaber, etwa über Download-Optionen. Diese Bereitstellungspflicht gilt auch heute schon, sie greift seit dem 12. September 2025.

Unmittelbar berechtigt ist der Nutzer. Das ist nach Art. 3 Nr. 12 Data Act jede „natürliche oder juristische Person, die ein vernetztes Produkt besitzt oder der vertraglich zeitweilige Rechte für die Nutzung des vernetzten Produkts übertragen wurden oder die verbundenen Dienste in Anspruch nimmt".

Der Data Act legt die faktische Hoheit über die von der eigenen Nutzung generierten Daten damit ausdrücklich zum Anwender – sei es als Eigentümer, Mieter, Leasingnehmer oder Service-Kunde. Zugleich darf der Nutzer eine Weitergabe der Daten an Dritte erlauben, etwa an Werkstätten, Dienstleister oder Innovationspartner. Diese Dritten sind im Sprachgebrauch des Data Act „Datenempfänger".

Der Nutzer muss nicht notwendigerweise die betroffene Person sein, auf die sich entsprechende Nutzungsdaten beziehen. Dies fällt beispielsweise regelmäßig im Fall von Mietwagen, Dienstwagenflotte oder industriellen Maschinen mit Login der Arbeitnehmer auseinander, denn in all diesen Fällen wird der Vermieter oder Arbeitgeber „Nutzer" sein, betroffene Person aber Fahrer oder Maschinenführer.

Spannungsverhältnis zum Datenschutzrecht

Wenn sich der Datenzugang auf personenbezogene Daten bezieht, führt die Regelung in Art. 1 Abs. 5 Satz 1 Data Act, nach der die DSGVO „unbeschadet" bleibt, zu einem herausfordernden Befund: Der Datenzugang muss vollständig datenschutzkonform erfolgen. Dies bedeutet insbesondere, dass jeder Datenzugang zugunsten des Nutzers und jede Weitergabe an einen Datenempfänger einer eigenständigen Legitimation nach der DSGVO bedarf, wenn und soweit es sich um personenbezogene Daten handelt. Erwägungsgrund 7 Data Act hält insofern eindeutig fest, dass der Data Act selbst „keine Rechtsgrundlage für die Erhebung oder Generierung personenbezogener Daten durch den Dateninhaber" enthält. Eine Verarbeitungserlaubnis aus Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO i.V.m. dem Data Act entfällt damit.

In der Praxis bedeutet das: Nutzer, Dateninhaber und Datenempfänger stehen vor der Aufgabe, die datenschutzrechtliche Legitimation für die Verarbeitung personenbezogener Daten – etwa Vertragserfüllung, Interessenabwägung oder Einwilligung – jeweils zu prüfen und rechtssicher zu dokumentieren. Die Herausforderungen liegen im Zusammenspiel von Nutzer- und Betroffeneneigenschaft und der operativen Umsetzung, wenn mehrere Personen (Mitarbeitende, Kunden, Besucher) auf sie beziehbare Daten generieren.

Eine Entscheidung, bei datenschutzrechtlichen Zweifeln auf die weitere Verarbeitung zu verzichten, ist dabei im Anwendungsbereich des Data Act nicht möglich: Besteht eine datenschutzrechtliche Erlaubnisgrundlage, greift das Datenzugangsrecht nach Data Act und der Datenzugang ist verpflichtend zu gewähren. Besteht keine datenschutzrechtliche Erlaubnis, darf der Datenzugang nicht gewährt werden.

Datenschutzrechtliche Erlaubnisgrundlagen für den Datenzugang nach Data Act

Für die Bereitstellung und Weiterleitung von Nutzungsdaten nach dem Data Act können alle datenschutzrechtlichen Erlaubnisgrundlagen herangezogen werden. Dabei ergeben sich allerdings einige typischen Konstellationen:

- Die Erlaubnis der Vertragserfüllung (Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO) ist regelmäßig nur relevant, wenn Nutzer und Betroffener identisch sind. Denn bekanntlich muss für diese Erlaubnisgrundlage der Vertrag zwischen Betroffenem und Verantwortlichem bestehen. Ein relevanter Fall dieser Erlaubnis ist etwa die Anforderung des Nutzers und Betroffenen gegenüber dem Dateninhaber, die Fahrdaten seines Autos an die Werkstatt zu übermitteln.
- Denkbar ist auch der Weg über eine Einwilligung (Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO), die allerdings nur für Einzelfälle handhabbar ist, insbesondere aber im Beschäftigtenverhältnis oder bei Massenkonstellationen schnell an praktische Grenzen stößt.
- Häufig in der Praxis relevant wird der Weg über die berechtigten Interessen der beteiligten Akteure (Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO). Hier ist eine umfassende, vorab dokumentierte Interessenabwägung durchzuführen. Elementar ist hierfür die immer erforderliche Betroffeneninformation, da darüber – jedenfalls bei deutlicher Hervorhebung – auch eine entsprechende Erwartungshaltung der Betroffenen erzeugt werden kann (Erwägungsgrund 47 DSGVO). Nicht tragfähig ist dieser Weg allerdings für die Verarbeitung sensitiver Daten i.S.d. Art. 9 DSGVO, etwa über eine Fitness-App. In diesen Fällen ist häufig nur der Weg über die Einwilligung gangbar.

Daneben müssen alle weiteren datenschutzrechtlichen Anforderungen eingehalten werden, einschließlich der Rechenschaftspflichten nach Art. 5 Abs. 2 DSGVO und einer angemessenen Datensicherheit gemäß Art. 32 DSGVO. Zu erwägen sind bei alledem auch der Einsatz von Privacy Enhancing Technologies (PETs) im Rahmen der Datengenerierung. Diese führen dazu, dass zunächst personenbezogene Daten unmittelbar durch technische Maßnahmen geschützt werden - etwa durch Pseudonymisierung oder Anonymisierung. Umstritten war daher, ob diese Daten dann nicht mehr dem Datenzugangsrecht unterfallen, weil sie durch den Einsatz der PETs verändert werden, der Datenzugang aber nur auf die Nutzungsdaten in Rohform abzielt. Dieser Ansicht hat die EU-Kommission allerdings eine Absage erteilt: Auch die nach dem Einsatz von PETs datenschutzfreundlicheren Daten unterliegen dem Datenzugangsrecht. PETs werden nach Nr. 13 der FAQ der EU-Kommission zum Data Act nicht als Verarbeitungseinrichtungen verstanden, die dazu führen würden, dass es sich bei den so bearbeiteten Daten nicht mehr um dem Datenzugangsrecht unterliegende Rohdaten handeln würde (FAQ Data Act, Version 1.4 v. 22.01.2026, S. 12).[3]

Vertragsgestaltung

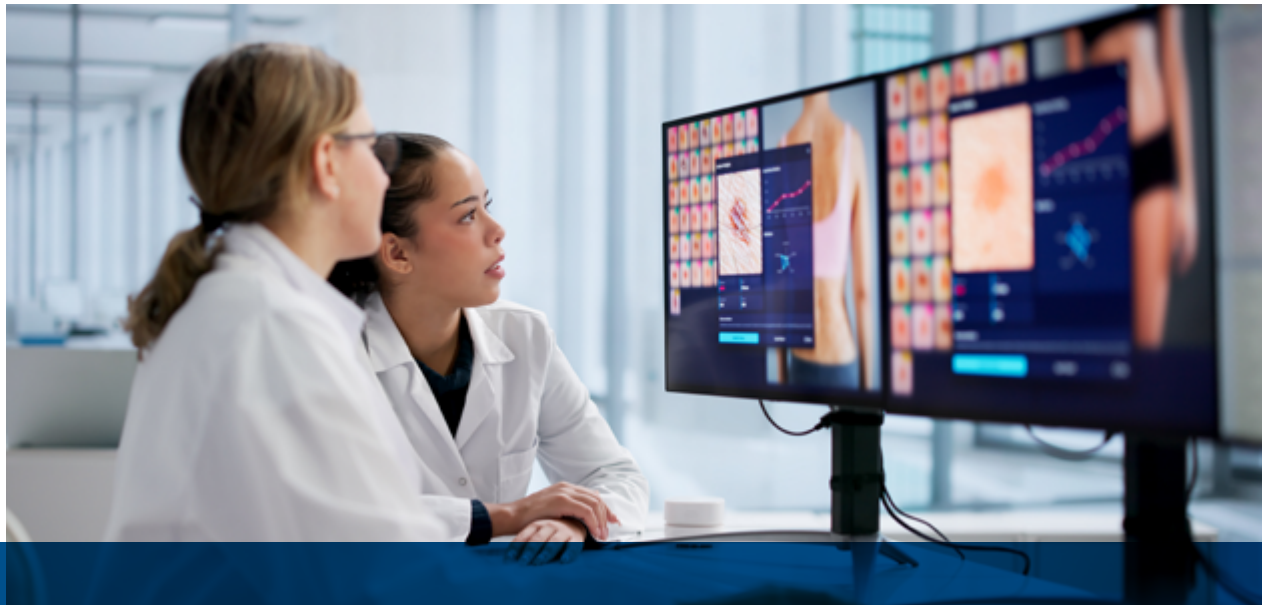
Der Data Act verpflichtet Unternehmen dazu, Datennutzungsverträge abzuschließen, wenn Dritte Zugriff auf durch vernetzte Produkte generierte Daten verlangen oder erhalten, der Nutzer also die Bereitstellung der Daten an einen Datenempfänger verlangt. Zudem dürfen Dateninhaber und Hersteller Nutzungsdaten nur noch verwenden, wenn der Nutzer dies vertraglich erlaubt – zumindest, soweit es sich um nicht-personenbezogene Daten handelt. Ob dies auch für personenbezogene Daten gilt, ist umstritten; teleologisch sollte für diese kein geringerer Schutzgrad gelten.

Ziel der Notwendigkeit von Datennutzungsverträgen ist es, die Rahmenbedingungen für Datenzugang, -nutzung und -weitergabe klar und transparent zu regeln. Um die Vertragsgestaltung zu erleichtern, muss die EU-Kommission gemäß Art. 41 Data Act Model Contractual Terms („MCT") vorlegen. Die erste Fassung der MCTs ist im November 2025 verabschiedet worden.[4] Die MCTs stellen unverbindliche Empfehlungen dar. Sie zielen darauf ab, Mindeststandards für Datenidentifikation, Nutzungsrechte, Vergütung und die Behandlung von Geschäftsgeheimnissen festzulegen.

In Sachen Datenschutz enthalten die Model Contractual Clauses lediglich allgemeine Hinweise zum Schutz personenbezogener Daten und zur Einhaltung der DSGVO. Konkrete vertragliche Regelungen zur Umsetzung des Datenschutzrechts oder auch zur Auftragsverarbeitung (AVV), gemeinsamen Verantwortung (Joint Controllership Agreement, JCA) oder zur datenexportbezogenen Absicherung fehlen. Vielmehr wird auf die eigenständige Umsetzung der datenschutzrechtlichen Vorgaben außerhalb dieser Musterklauseln verwiesen; Datenschutzverträge sind somit gesondert zu erstellen und zu vereinbaren.

[3] Abrufbar unter https://digital-strategy.ec.europa.eu/de/library/commission-publishes-frequently-asked-questions-about-data-act

[4] Abrufbar unter https://digital-strategy.ec.europa.eu/en/library/draft-recommendation-non-binding-model-contractual-terms-data-access-and-use-and-non-binding (Links zuletzt abgerufen am 28.02.2026).



Gerade weil die MCT keine vollwertigen Regelungen zur Auftragsverarbeitung oder für Fälle gemeinsamer Verantwortlichkeit enthalten, bleibt eine spezifische datenschutzrechtliche Vertragsanpassung erforderlich, wenn über die Datennutzung hinaus eine Verarbeitung personenbezogener Daten erfolgt. Zu unterscheiden sind drei typische Fallgestaltungen:

- Dateninhaber und Datenempfänger agieren unabhängig: Keine AVV oder JCA erforderlich; eine konkrete Festlegung von Rechten und Pflichten zur DSGVO-Compliance sollte aber geprüft werden und ist je nach konkretem Einzelfall ratsam.
- Gemeinsame Festlegung der Zwecke und Mittel der Datenverarbeitung durch Dateninhaber und Nutzer oder auch Nutzer und Datenempfänger oder Dateninhaber und Datenempfänger: Abschluss eines Vertrags zur gemeinsamen Verantwortung nach Art. 26 DSGVO notwendig.
- Datenverarbeitung im Auftrag: Auftragsverarbeitungsvertrag (AVV) nach Art. 28 DSGVO muss vereinbart werden; ein „Dateninhaber" kann indes nie Auftragsverarbeiter sein, da er dann mangels eigenständiger Entscheidungsbefugnisse per definitionem kein Dateninhaber mehr wäre (Erwägungsgrund 22 Data Act).
- Drittstaatenübermittlung: Absicherung des Datenschutzniveaus im Zielland, unter Umständen mit Standardvertragsklauseln der EU-Kommission 2021/914/EU oder entsprechenden Maßnahmen nach Art. 44 ff. DSGVO.

Umsetzung in der Praxis – Zusammenarbeit von Datenschutzbeauftragten und Data Act-Zuständigen

Um den Datenzugangsanspruch nach dem Data Act datenschutzkonform abzusichern, sollten in der Praxis folgende Aspekte beachtet werden:

- Prüfung, ob und welche personenbezogenen Daten im Kontext des Datenzugangs ausgetauscht werden.
- Identifikation der datenschutzrechtlichen Rollen (Verantwortlicher, gemeinsam Verantwortliche, Auftragsverarbeiter).
- Ergänzende Datenschutzvereinbarungen, abhängig von der Rolle der Akteure (AVV, JCA, Standarddatenschutzklauseln).
- Sicherstellung der DSGVO-Konformität, von der Erlaubnisgrundlage über die Zweckbindung bis zur Datenminimierung, einschließlich Aktualisierung der relevanten Betroffeneninformationen.
- Besondere Aufmerksamkeit verdient die Datensicherheit nach Art. 32 DSGVO, die auch beim Datenzugang gewährt sein muss.
- Häufig wird der Datenzugangsanspruch schließlich im Verzeichnis der Verarbeitungstätigkeiten neu oder in bestehenden Prozessen ausdrücklich abzubilden sein, womöglich ist auch eine Datenschutz-Folgenabschätzung erforderlich.

Behördenzuständigkeit und Durchsetzung

Wie beim Vollzug von EU-Rechtsakten üblich, wird auch die Durchsetzung des Data Act durch nationale Behörden in den Mitgliedstaaten erfolgen. Artikel 37 des Data Act sieht dazu eine zweigeteilte Behördenzuständigkeit vor: nämlich die grundzuständige Behörde nach Absatz 1 der Norm und daneben nach Absatz 3 eine Zuständigkeit der „für die Überwachung der Anwendung der Verordnung (EU) 2016/679 [DSGVO] zuständigen Aufsichtsbehörden" soweit es um den

Schutz personenbezogener Daten geht. Über Art. 37 Abs. 3 Data Act werden die nach der DSGVO benannten Datenschutzaufsichtsbehörden so auch „für die Überwachung" des Data Act zuständig.

Die Benennung der nach Art. 37 Abs. 1 Data Act zuständigen Behörde steht in Deutschland noch aus: Das Data Act-Durchführungsgesetz liegt bislang nur im Entwurf vor und durchläuft aktuell das parlamentarische Verfahren (BT-Dr. 21/2998, zuletzt im Januar 2026 mit Änderungsvorschlägen insbesondere vom Bundesrat). Grundzuständige Behörde soll danach die Bundesnetzagentur (BNetzA) werden. Umstritten ist – und maßgeblicher Grund für die verzögerte Umsetzung –, wer die Datenschutzaufsicht übernehmen soll: Die nach der DSGVO benannten 17 Datenschutzaufsichtsbehörden in den Bundesländern je nach ihrem Zuständigkeitsbereich oder zentral die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) in Bonn? Letzteres wird nunmehr vorgeschlagen, um für die Wirtschaft einen einheitlichen Anlaufpunkt zu etablieren. EU-rechtlich wird dagegengehalten, dass durch den Verweis des Art. 37 Abs. 3 Data Act auf die DSGVO der deutsche Gesetzgeber hier keinen Spielraum habe, sondern den nach dem deutschen Datenschutzrecht zuständigen Behörden auch die Data Act-Zuständigkeit überlassen muss, also föderal differenziert allen 17 Datenschutzaufsichtsbehörden. Letztlich belässt aber auch die DSGVO dem nationalen Gesetzgeber Spielraum, welchen nationalen Aufgaben er in Sachen Datenschutz welche Aufgabe zuweist. Schon heute setzen die nach der DSGVO benannten Behörden den Data Act um, erste Verfahren sind anhängig, und zwar nicht nur gegen die Gewährung auf Datenzugang, sondern auch mit der Argumentation, dass eine Erlaubnisgrundlage nach DSGVO bestehe und daher der Datenzugang nach Data Act zu gewähren ist.

Im Fall von Verstößen gegen den Data Act sind die Aufsichtsbehörden befugt, diesen durchzusetzen, also etwa einen Datenzugang anzuordnen. Darüber hinaus können Bußgelder verhängt werden. Die Bußgeldmechanismen des Data Act orientieren sich an den aus der DSGVO bekannten Vorgaben.

Entbürokratisierung durch den Digital-Omnibus?

Im November 2025 hat die EU-Kommission mit dem „Digital Package on Simplification on digital acquis" (COM(2025) 837 final) einen Vorschlag zur Überarbeitung unter anderem des Data Act vorgelegt. Ziel ist es, die zunehmende Komplexität der digitalen Gesetzgebung zu reduzieren und die Kohärenz innerhalb des EU-Rechtsrahmens zu stärken. Die Omnibus-Initiative sieht koordinierte Anpassungen mehrerer zentraler Rechtsakte vor – darunter neben dem Data Act insbesondere auch der DSGVO.

Das Verhältnis der beiden Rechtsakte zueinander wird indes auch in dem jetzt vorliegenden Änderungsvorschlag nicht neu geregelt. Der Data Act soll allerdings zum umfassenden Datengesetzbuch ausgebaut werden und unter anderem den Data Governance Act und die Verordnung zum freien Fluss nicht-personenbezogener Daten mit aufnehmen. Die Parallelität zur DSGVO wird allerdings unverändert bestehen bleiben und damit auch die heute schon bestehenden Herausforderungen der datenschutzkonformen Gewährung des Datenzugangs nach Data Act.

AUSBLICK

Der Data Act markiert regulatorisch eine umfassende Neuausrichtung der Regulierung der Datenwirtschaft. Daten werden zur geteilten Ressource, die wirtschaftlich und gesellschaftlich genutzt – aber auch rechtlich und technisch abgesichert – werden muss.

Unternehmen sollten Compliance, Technik und Rechtsfragen gerade im Spannungsfeld von Data Act und DSGVO zusammendenken. Ob sich dieser regulatorische Kontinentalbruch auch in der Praxis verwirklichen wird, bleibt indes abzuwarten. Die Relevanz des Data Act im Markt ist derzeit noch begrenzt, wohl auch, weil eine klare Behördenzuständigkeit in Deutschland noch aussteht.

Über die Autorin

Dr. Kristina Schreiber
ist Rechtsanwältin, CIPP/E, Fachanwältin für Verwaltungsrecht und Partnerin bei Loschelder Rechtsanwälte in Köln. Sie ist spezialisiert auf die rechtliche Begleitung von Digitalisierungsprojekten, von der App über individuelle Softwareprojekte bis hin zu Datennutzungsstrategien. Kristina Schreiber bloggt auf www.digitalisierungsrecht.eu und publiziert regelmäßig zu diesen Themen, unter anderem ist sie Herausgeberin des Praxishandbuchs Softwarerecht im Beck-Verlag, bis zur 7. Auflage bekannt als „der Marly", Mitautorin des Buches "KI und Recht für Dummies" und hat einen Einführungsband zum Data Act mit verfasst, der im Nomos Verlag erschienen ist.