Digitalisierung

Data Act

vbw

Leitfaden
Stand: September 2024

Die bayerische Wirtschaft

Hinweis

Vorwort

Data Act bringt neue Möglichkeiten und Anforderungen für Unternehmen.

Durch die tägliche private und wirtschaftliche Nutzung von smarten und vernetzten Geräten entstehen große Datenmengen. Einerseits ist es wichtig, Persönlichkeitsrechte und Geschäftsgeheimnisse zuverlässig zu schützen. Andererseits gilt es anzuerkennen, dass Daten unter Einhaltung fairer Nutzungsbedingungen eine wichtige Ressource sind und erhebliche Wertschöpfungspotenziale noch brachliegen. Ein eindeutiges Regelwerk ist daher unabdingbar für eine wettbewerbsfähige Datenwirtschaft.

Als erstes Ergebnis der europäischen Datenstrategie dient der Data Act der Harmonisierung der Vorschriften für Datenzugang und Datennutzung. Alle Akteure in der Wertschöpfungskette vernetzter Geräte – insbesondere aber deren Nutzer – sollen von den entstehenden Daten profitieren können. So stellt der Data Act Regeln für den Zugriff auf Daten, Vertragsklauseln, Wechsel von Datenverarbeitungsdiensten und Förderung der Interoperabilität auf. Herausforderungen ergeben sich etwa aus dem Zusammenspiel mit dem Datenschutzrecht.

Mit dem Leitfaden *Data Act* unterstützen wir Unternehmen beim Umgang mit der veränderten Rechtslage. Er erläutert die Anforderungen und gibt Handlungsempfehlungen zur Gestaltung entsprechender Anpassungsmaßnahmen. Zudem werden Schnittstellen mit der KI-Verordnung und Besonderheiten bei der Datennutzung durch KI-Systeme betrachtet.

Bertram Brossardt
30. September 2024

Inhalt

1 Einleitung

Regulierung der vernetzten Datenwirtschaft

Die fortschreitende Technologisierung mit der Nutzung von „smarten Geräten“ sorgt für eine **wachsende Vernetzung** und eine zunehmende Produktion von Informationen bzw. Daten. Wearables wie eine Smartwatch, smarte Kühlschränke, TV-Geräte oder vernetzte Fahrzeuge produzieren bei ihrer Verwendung durch den jeweiligen Nutzer diverse Daten über verschiedene Sensoren. Diese Daten dienen zunächst einmal der Gewährleistung bestimmter Funktionen des Produkts und werden darüber hinaus – wenn überhaupt – oft nur vom Hersteller des Produktes ausgewertet, weil nur dieser Zugriff auf diese Gerätedaten hat.

Die Europäische Union hat ein Bündel an Maßnahmen ergriffen, um diese Daten (besser) nutzbar zu machen. Diese Maßnahmen sollen insgesamt zur **Stärkung der Datenwirtschaft in der EU** beitragen. Bislang nehmen die Datenmengen in der EU stetig zu. Es werden dabei allerdings nur 20 % dieser Daten genutzt.[1] Bis 2028 könnten Schätzungen zufolge mit den neuen Regeln bis zu 270 Milliarden Euro zusätzlich erwirtschaftet werden.[2]

Einen wesentlichen Baustein hierfür bildet die **Datenverordnung** (Data Act; VO (EU) 2023/2854), im Folgenden wird die in der Praxis verwendete englische Fassung zugrundegelegt: **Data Act**.[3] Der Data Act wurde in Ergänzung speziell zum Data Governance Act (DGA) erlassen. Während der DGA auf einen freiwilligen Datenaustausch (Datenaltruismus) setzt, etabliert der Data Act verbindliche rechtliche Ansprüche in Bezug auf den Zugriff und die Nutzung von Daten. Ziel des Data Acts ist es, alle Akteure in einer Wertschöpfungskette vernetzter Geräte von den Daten profitieren zu lassen, die durch die Nutzung solcher Geräte oder durch die Verwendung verbundener Dienste entstehen. Die Datenwirtschaft in der EU soll insgesamt verbessert werden und es soll ein wettbewerbsfähiger Datenmarkt gefördert werden. Daten sollen zugänglicher und nutzbarer gemacht werden, um Innovation zu fördern. Gleichzeitig soll die Verteilung der Daten nach dem Prinzip der Fairness erfolgen.[4] Insgesamt regelt der Data Act, welcher Akteur welche Daten zu welchen Bedingungen nutzen darf.[5] Dabei steht die Kontrolle der Daten durch den Nutzer eines vernetzten Gerätes im Vordergrund.

---

[1] Köllner, Das bedeutet der EU Data Act für Connected Cars, https://www.springerprofessional.de/automobilwirtschaft/datenmanagement/das-bedeutet-der-eu-data-act-fuer-connected-cars/20191550.
[2] Köllner, Das bedeutet der EU Data Act für Connected Cars, https://www.springerprofessional.de/automobilwirtschaft/datenmanagement/das-bedeutet-der-eu-data-act-fuer-connected-cars/20191550.
[3] Paschke, Datenrecht, in: Heckmann/Paschke, juris Praxiskommentar Internetrecht, 8. Aufl. 2024, Kap. 10 Rn. 48 ff.
[4] EU-Kommission, Erklärung zum Datengesetz, https://digital-strategy.ec.europa.eu/de/node/12633/printable/pdf, S. 1.
[5] EU-Kommission, Erklärung zum Datengesetz, https://digital-strategy.ec.europa.eu/de/node/12633/printable/pdf, S. 1.

2 Überblick

Vom Datenschutz zum Datenwirtschaftsrecht

Der Data Act ist am 11.01.2023 in Kraft getreten; seine Vorschriften gelten ab dem 12.09.2025.[6]

Abbildung 1
Datenbereitstellung vor und nach dem Data Act

Der Data Act regelt Rechte und Pflichten vor allem für drei typischerweise vorkommende Konstellationen, nämlich das Verhältnis zwischen

- **Unternehmen und Verbrauchern** wie etwa dem Hersteller eines vernetzten Produktes und dem privaten Nutzer des Gerätes (**B2C**)
- **Unternehmen untereinander** wie etwa dem Hersteller und einem dritten Datenempfänger (**B2B**)
- **Unternehmen und Behörden** wie etwa dem Hersteller und bestimmten Behörden im Falle eines Notstandes (**B2G**).

Sachlich stellt der Data Act vor allem Regeln für den Zugriff auf Daten, Vertragsklauseln, Wechsel von Datenverarbeitungsdiensten und Förderung der Interoperabilität für Teilnehmer an europäischen Datenräumen auf.

[6] ABl. L 2023/2854 vom 22.12.2023.

Einen ersten Eindruck von den Schwerpunkten des Data Acts bietet bereits ein auszugsweiser **Überblick über die einzelnen Hauptkapitel**:

Überblick zu den Regelungsschwerpunkten des Data Acts

Kapitel II	Datenweitergabe von Unternehmen an Verbraucher und zwischen Unternehmen
Kapitel III	Pflichten der Dateninhaber bei Weitergabe von Daten
Kapitel IV	Missbräuchliche Vertragsklauseln in Bezug zu Datenzugang und Datennutzung zwischen Unternehmen
Kapitel V	Bereitstellung von Daten für öffentliche Stellen bei außergewöhnlicher Notwendigkeit
Kapitel VI	Wechsel zwischen Datenverarbeitungsdiensten
Kapitel VII	Unrechtmäßiger Zugang zu nicht-personenbezogenen Daten im internationalen Umfeld
Kapitel VIII	Interoperabilität

Die **Ziele der Datenverordnung** werden in den Erwägungsgründen zum Data Act (im Folgenden nur: ErwG.), insbesondere Nr. 1, 2 und 4, formuliert. Danach soll die Regulierung einen **fairen Zugang zu Daten** schaffen und die **Nutzung dieser Daten in der digitalen Wirtschaft** vereinfachen. Bislang bestehen viele rechtliche Unsicherheiten im Kontext der Datenweitergabe. Diese sollen verringert werden.

In den letzten Jahren haben datengetriebene Technologien **transformative Wirkung auf alle Wirtschaftssektoren** gehabt. Insbesondere die rasche Verbreitung von Produkten, die mit dem Internet vernetzt sind, hat den Umfang und den potenziellen Wert von Daten für Verbraucher, Unternehmen und Gesellschaft erhöht. Hochwertige und interoperable Daten aus verschiedenen Bereichen steigern die Wettbewerbsfähigkeit und Innovation und sorgen für ein nachhaltiges Wirtschaftswachstum. Dieselben Daten können unbegrenzt für verschiedene Zwecke verwendet und weiterverwendet werden, ohne dass dadurch Qualität oder Quantität beeinträchtigt wird (ErwG. 1).

Hindernisse bei der Datenweitergabe verhindern jedoch eine optimale Verteilung der Daten zum Nutzen der Gesellschaft. Zu diesen Hindernissen gehören aus Sicht des europäischen Gesetzgebers

- der Mangel an Anreizen für Dateninhaber, freiwillig Vereinbarungen über die Datenweitergabe einzugehen,
- Unsicherheiten in Bezug auf Rechte und Pflichten in Verbindung mit Daten,
- die Kosten der Auftragsvergabe in Bezug auf technische Schnittstellen und für deren Einrichtung,
- die starke Fragmentierung von Informationen in Datensilos,
- die schlechte Verwaltung von Metadaten,
- fehlende Normen für die semantische und technische Interoperabilität,

– Engpässe beim Datenzugang,
– das Fehlen einheitlicher Verfahren für die Datenweitergabe und
– vertragliche Ungleichgewichte hinsichtlich Datenzugang und Datennutzung (ErwG. 2).

Um den **Bedürfnissen der digitalen Wirtschaft** gerecht zu werden und die Hindernisse für einen reibungslos funktionierenden Binnenmarkt für Daten zu beseitigen, soll ein harmonisierter Rahmen geschaffen werden, in dem festgelegt wird, wer unter welchen Bedingungen und auf welcher Grundlage berechtigt ist, Produktdaten oder verbundene Dienstdaten zu nutzen. Daher sollten die Mitgliedstaaten in den Angelegenheiten, die in den Anwendungsbereich der vorliegenden Verordnung fallen, keine zusätzlichen nationalen Anforderungen annehmen oder aufrechterhalten, sofern das in der vorliegenden Verordnung nicht ausdrücklich vorgesehen ist, da dies ihre direkte und einheitliche Anwendung beeinträchtigen würde. Ferner sollten auf Unionsebene ergriffene Maßnahmen die Verpflichtungen und Zusagen, die sich aus den von der Union geschlossenen internationalen Handelsabkommen ergeben, unberührt lassen (ErwG. 4).

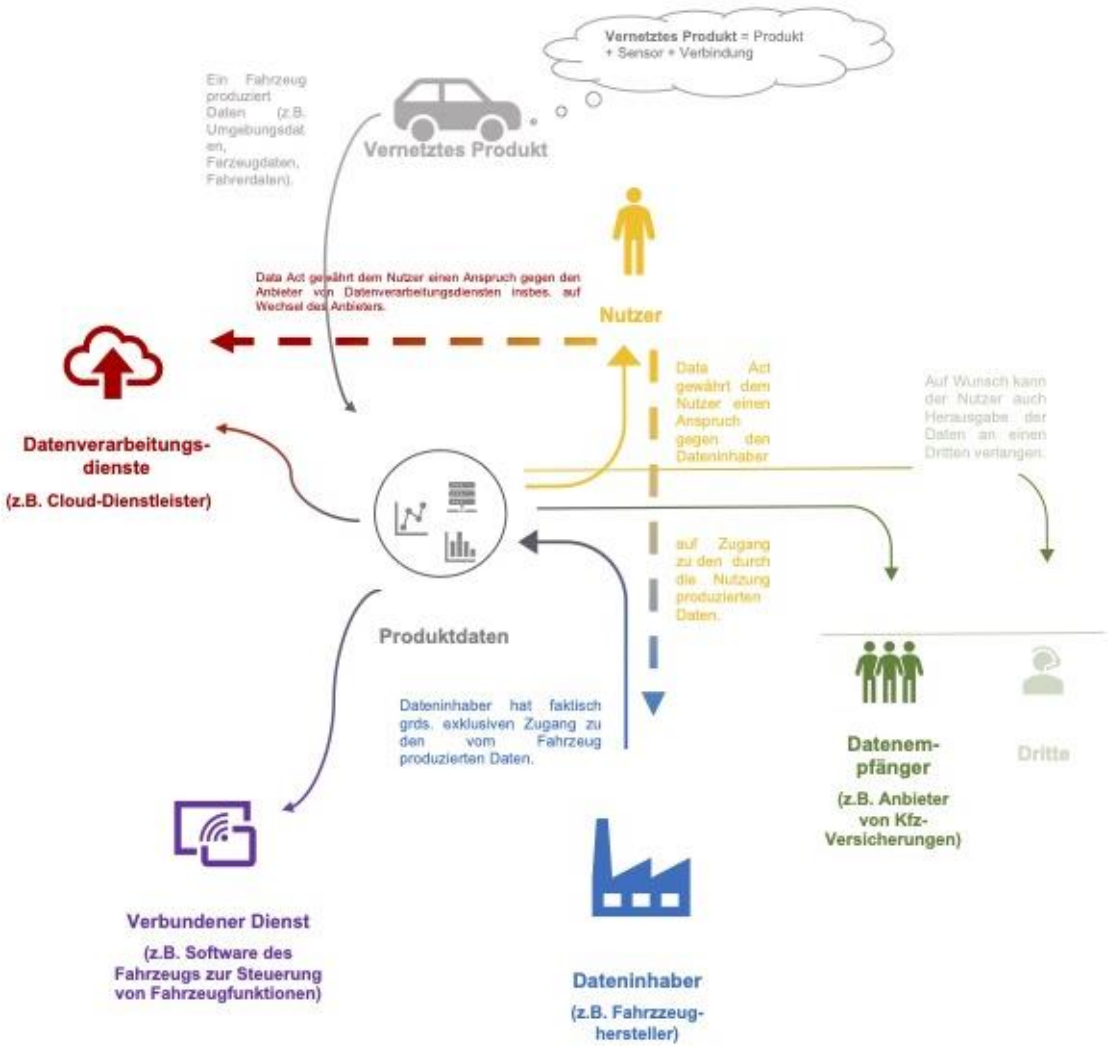
Die Datenverordnung führt bestimmte **Begrifflichkeiten** wie „Dateninhaber“, „Datenempfänger“ oder „verbundene Dienste“ neu ein, auf die im Folgenden eingegangen wird. Festzuhalten bleibt vorab, dass die Datenverordnung **sämtliche Arten von Daten** erfasst, unabhängig davon, ob es sich um personenbezogene Daten handelt.

– **Nutzer** ist eine natürliche oder juristische Person, die ein vernetztes Produkt besitzt oder der vertraglich zeitweilige Rechte für die Nutzung des vernetzten Produkts übertragen wurden oder die die verbundenen Dienste in Anspruch nimmt (Art. 2 Nr. 12 Data Act)[7].
– **Dateninhaber** ist eine 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 (Art. 2 Nr. 13 Data Act).
– **Datenempfänger** ist eine natürliche oder juristische Person, die zu Zwecken innerhalb ihrer gewerblichen, geschäftlichen, handwerklichen oder beruflichen Tätigkeit handelt, ohne Nutzer eines vernetzten Produktes oder verbundenen Dienstes zu sein, und dem vom Dateninhaber Daten bereitgestellt werden, einschließlich eines Dritten, dem der Dateninhaber auf Verlangen des Nutzers … Daten bereitstellt (Art. 2 Nr. 14 Data Act)
– **Datenverarbeitungsdienst** ist eine digitale Dienstleistung, die einem Kunden bereitgestellt wird und einen flächendeckenden und auf Abruf verfügbaren Netzzugang zu einem gemeinsam genutzten Pool konfigurierbarer, skalierbarer und elastischer Rechenressourcen ermöglicht (Art. 2 Nr. 8) Data Act.
– **Verbundener Dienst** ist ein digitaler Dienst, der so mit dem Produkt verbunden ist, dass das vernetzte Produkt ohne ihn eine oder mehrere seiner Funktionen nicht ausführen könnte oder der anschließend vom Hersteller oder einem Dritten mit dem Produkt verbunden wird, um die Funktionen des vernetzten Produkts zu ergänzen, zu aktualisieren oder anzupassen (Art. 2 Nr. 6 Data Act).

[7] Der Data Act bietet damit nicht nur Verbrauchern die Möglichkeit zum Datenzugang, sondern auch Unternehmen. Denn gerade die Unternehmen dürften diejenigen sein, die mit den Daten innovativ umgehen und ein Ziel des Data Act erfüllen.

Zusammenfassend lassen sich die einzelnen Akteure und ihre Rollen nach dem Data Act grafisch vereinfacht darstellen. Einzelheiten hierzu in den folgenden Kapiteln.

Abbildung 2
Rollen und Akteure im Data Act



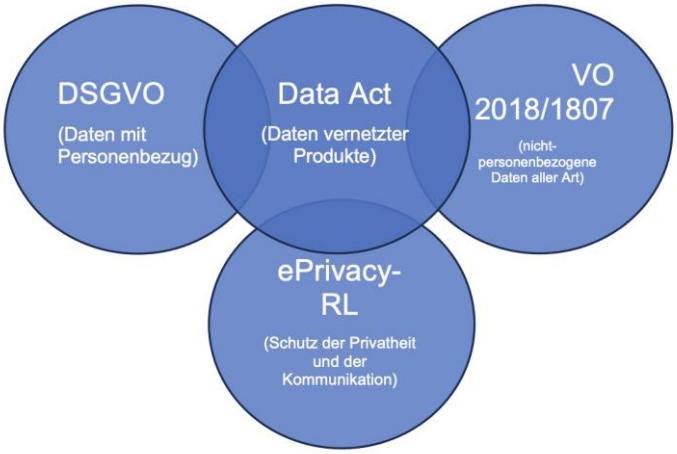
Quelle: © Dirk Heckmann

3 Der Data Act im rechtlichen Kontext

Europäische Datenregulierung

Der Data Act ist Teil der europäischen Datenstrategie. Er fügt sich in die bereits bestehenden Verordnungen und Richtlinien, insbesondere die zum Daten- und Privatheitsschutz, ein.

Abbildung 3
Data Act im Kontext weiterer Datengesetze



Quelle: © Dirk Heckmann

3.1 Verhältnis zu weiteren EU-Rechtsakten mit Datenbezug

In den letzten Jahren hat die EU den Umgang mit Daten in zahlreichen Rechtsakten näher reguliert. Am bekanntesten ist hierbei die Datenschutzgrundverordnung (DSGVO), die aber nur für personenbezogene Daten gilt. Daneben sind u. a. die VO (EU) 2018/1725 (Verordnung zum freien Verkehr nicht-personenbezogene Daten) und die ePrivacy-Richtlinie (RL 2002/58/EG, Richtlinie zum Schutz der Privatheit und der Kommunikation) zu nennen. Diese Rechtsakte lässt der Data Act „unberührt“ (ErwG. 7), sie (und weitere – siehe im Anschluss) bestehen gleichberechtigt nebeneinander, keine Verordnung oder Richtlinie verdrängt eine andere: „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.“

3.1.1 Data Act und DSGVO

Im Falle eines Widerspruchs zwischen dem Data Act und dem Datenschutzrecht ist letzterem der Vorrang einzuräumen (Art. 1 Abs. 5 Satz 3 Data Act).

Insofern stellen die Vorschriften des Data Act auch **„keine Rechtsgrundlage für die Erhebung oder Generierung personenbezogener Daten“** dar. Diese Formulierung in ErwG. 7 bedeutet jedoch nicht, dass die Regelungen aus dem Data Act keine Rechtsgrundlage für eine Verarbeitung personenbezogener Daten generell darstellen können. Abgesehen davon, dass Erwägungsgründe ohnehin nicht rechtsverbindlich sind, sondern eher als Auslegungshilfe dienen, ist dort die Rede von „Erhebung“ und „Generierung“. Der Verarbeitungsbegriff (Art. 4 Nr. 2 DSGVO) erfasst aber auch andere Verarbeitungsformen, etwa die **Datenübermittlung an einen Dritten**. Hierfür bietet der Data Act i.V.m. Art. 6 Abs. 1 lit. C DSGVO eine Rechtsgrundlage.

Gleichwohl sind die **Anforderungen der DSGVO** von zentraler Bedeutung, wenn es um die Verarbeitung personenbezogener Daten geht. So bedarf es eines datenschutzrechtlichen Rechtfertigungstatbestands, der sich aus Art. 6 bzw. 9 DSGVO ergeben muss. Genauso haben die Datenschutzgrundsätze aus Art. 5 DSGVO Geltung, worauf ErwG. 8 hinweist.

Hinsichtlich der Verarbeitung personenbezogener Daten werden die **Betroffenenrechte** erweitert[8], das bedeutet: Der Nutzer hat nicht nur den Auskunftsanspruch nach Art. 15 DSGVO oder das Recht auf Datenübertragbarkeit nach Art. 20 DSGVO, sondern umfangreiche Ansprüche auf Information (siehe Art. 3 Data Act) oder Datenherausgabe (Art. 4 und 5 Data Act). Der Data Act stärkt damit die ohnehin schon starke Position derjenigen, um deren personenbezogene Daten es geht.

Zusammengefasst: Der Data Act erweitert den Zugriff aus personenbezogene Daten gegenüber der DSGVO nicht. Soweit aber solche Daten datenschutzkonform einmal erhoben wurden, erleichtert der Data Act die **Partizipation an diesen Daten**, insbesondere deren Weiterleitung – dies natürlich nur im Rahmen der Anforderungen, die im Data Act für die verschiedenen Nutzungsformen normiert sind.

Beispiel: Zugang zu Fahrzeugdaten

Die Auto AG als Herstellerin vernetzter Fahrzeuge verarbeitet diverse Fahrzeugdaten. Die Halterin und Nutzerin eines Fahrzeugs der Auto AG verlangt Zugang zu den erzeugten Fahrzeugdaten gemäß Art. 3 Abs. 1 Data Act. Die Auto AG muss hierbei nicht nur die Pflicht aus Art. 3 Abs. 1 Data Act beachten und darf die Daten ohne Weiteres herausgeben, sondern muss gleichzeitig prüfen, ob die DSGVO dies erlaubt, da die speziell auf die Halterin und Nutzerin bezogenen Daten in den Anwendungsbereich der DSGVO fallen.

[8] Art. 1 Abs. 5 Satz 2 Data Act.

Die Auto AG kann die Übermittlung der Daten, die sich auf die Halterin und Nutzerin beziehen, in diesem Fall sowohl auf den Rechtsgrund aus Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO („gesetzliche Pflicht“) i.V.m. Art. 3 Abs. 1 Data Act als auch auf Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO („Einwilligung“) stützen.

Die Pflicht aus Art. 3 Data Act gibt der Auto AG jedoch nicht das Recht, ergänzend Fahrerprofildaten für den Fall zu erheben, in dem es unterschiedliche Fahrer gibt. Die Auto AG kann allein aus Art. 3 Abs. 1 Data Act nicht herleiten, jeden Fahrer zur Erstellung eines eigenen Fahrerprofils zu verpflichten. Für diese Erhebung personenbezogener Daten muss die Auto AG einen eigenen Rechtsgrund haben, der sich aber gerade nicht aus Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO i.V.m. Art. 3 Abs. 1 Data Act ergibt. Die Erhebung verschiedener Fahrerprofile kann allerdings etwa auf entsprechende Einwilligungen (6 Abs. 1 UAbs. 1 lit. a DSGVO) oder ein berechtigtes Interesse (6 Abs. 1 UAbs. 1 lit. f DSGVO) gestützt werden, sofern die jeweiligen Voraussetzungen vorliegen.

Praxishinweis: Zuordenbarkeit personenbezogener Daten als Unternehmenspflicht?

Aus Art. 3 Data Act ergibt sich eine Verpflichtung für Unternehmen, Daten so zu speichern/bereitzustellen, dass diese *„für den Nutzer einfach, sicher, unentgeltlich in einem umfassenden, strukturierten, gängigen und maschinenlesbaren Format und, soweit relevant und technisch durchführbar, direkt zugänglich sind*“. Hier stellt sich die für Unternehmen die praktisch relevante Frage, ob man aus „strukturiert“ und „direkt zugänglich“ schließen kann, dass diese Daten im jeweiligen Kontext auch dem jeweiligen Betroffenen zuordenbar sein müssen? Die Erfüllung der **Bereitstellungspflicht könnte mit dem Grundsatz der Datenminimierung kollidieren**, wonach Unternehmen ja ein Interesse haben könnten, Daten zu anonymisieren, weil der Personenbezug für ihre eigenen Zwecke nicht (mehr) erforderlich ist.

Tatsächlich kann das Zugänglichmachen der Daten gem. Art. 3 Abs. 1 Data Act grds. i.S.v. Access by Design über einen Direktzugang des Nutzers erfolgen. Die Daten können aber auch alternativ erst auf Verlangen des Nutzers bereitgestellt werden, dann aber unverzüglich und *„falls relevant und technisch durchführbar – in der gleichen Qualität wie für den Dateninhaber kontinuierlich und in Echtzeit*“ (Art. 4 Abs. 1 Data Act). Da es im Rahmen des Data Acts letztlich um die Nutzbarkeit aller entsprechenden Daten gehen soll und die datenschutzrechtlichen Bestimmungen unberührt bleiben (ErwG. 7 Data Act**) gelten die Vorgaben der DSGVO wie das Prinzip der Datenminimierung weiterhin** vorrangig.

Im Kontext der Weitergabe von Daten an Dritte zieht der Data Act eine **Parallele zum datenschutzrechtlichen Recht auf Datenübertragbarkeit** (ErwG. 35 Data Act). Hier wird insbesondere genannt, dass der Data Act in dieser Hinsicht den Anspruch aus Art. 20 DSGVO ergänzt. Eine solche Parallele zieht der Data Act zu Art. 15 DSGVO hingegen nicht. Hieraus dürfte ebenfalls folgen, dass die Daten nicht zwingend zuordenbar zur Verfügung stehen müssen.

Schließlich besagt ErwG. 8 Data Act, dass die Datenschutzgrundsätze wie Datenminimierung auch im Kontext des Data Act eine große Bedeutung haben und auch **Maßnahmen wie Pseudonymisierung (und ggf. auch Anonymisierung) zur Anwendung kommen** sollen.

Praktisch dürfte dies folgendes bedeuten:
- Ermöglicht ein Dateninhaber einem Nutzer einen **unmittelbaren Zugang**, sobald die Daten entstehen, und sind diese Daten dann noch unmittelbar zuordenbar, dürfte dies der Intention des Data Acts in weitem Umfang Rechnung tragen und gleichzeitig auch mit den Prinzipien der DSGVO vereinbar sein.
- Ermöglicht ein Dateninhaber einem Nutzer einen **Zugang auf Anfrage** zu einem zeitlich späteren Zeitpunkt und hat der Dateninhaber die relevanten personenbezogenen Daten bis zu diesem Zeitpunkt bereits anonymisiert (etwa um sie umfassender und ohne Restriktionen aus dem Bereich des Datenschutzrechts für sich nutzen zu dürfen), dann trägt der Dateninhaber der DSGVO ebenso Rechnung und kommt damit zugleich den Anforderungen des Data Acts nach.

3.1.2 Data Act und Data Governance Act

Der **Data Governance Act (DGA)** findet neben dem Data Act Anwendung. Allerdings sind die Vorschriften aus dem Data Act zum Teil spezieller und abschließend. Wenn ein Dateninhaber gemäß Kapitel V Data Act öffentlichen Stellen Daten im Falle eines Notstandes bereitstellen muss, so gelten für diese Daten nicht die Vorschriften des DGA. Diese Daten sind insbesondere nicht zur Weiterverwendung i.S.d. Art. 3 ff. DGA bestimmt, sondern die jeweilige Stelle muss die Daten nach Erreichung des speziellen Zwecks löschen (Art. 19 Abs. 1 lit. c Data Act).

Der Data Act steht dem Abschluss darüberhinausgehender, **freiwilliger rechtmäßiger Verträge über die Datenweitergabe**, die seinen Anforderungen entsprechen, nicht entgegen (Art. 1 Abs. 10 Data Act), sondern schreibt lediglich ein Mindestmaß fest. Sowohl der DGA als auch der Data Act wollen die Datenwirtschaft insgesamt fördern, sodass ein größerer Datenaustausch stets zulässig ist, sofern keine anderen Gesetze dies verbieten.

3.1.3 Data Act und Datenverträge

Ebenso gilt der Data Act nicht für **freiwillige Vereinbarungen über den Datenaustausch zwischen privaten und öffentlichen Stellen** (Art. 1 Abs. 6 Data Act). Art. 14 ff. Data Act normieren lediglich die Pflicht zur Datenbereitstellung wegen außergewöhnlicher Notwendigkeit. Darüberhinausgehende Absprachen können getroffen werden.

Neben dem Datenschutzrecht dient der Data Act auch der Sicherstellung des **Verbraucherschutzes**. Die Vorschriften des Zivilrechts „über das Zustandekommen von Verträgen, ihre Gültigkeit oder ihre Rechtsfolgen oder über die Auswirkungen der Beendigung eines

Vertrages“ werden jedoch durch den Data Act insoweit nicht tangiert, als diese Verordnung keine spezifischen Regelungen dahingehend getroffen hat, ErwG. 9.

Ob und wie ein Vertrag zustande kommt (z. B. welche Form zu wahren ist), regelt der Data Act nicht, wohl aber welche Vertragsklauseln nicht vereinbart werden dürfen und verboten sind. Ausdrückliche vertragliche Regelungen enthält der Data Act in Art. 13, in dem missbräuchliche Vertragsklauseln in Bezug auf den Datenzugang und die Datennutzung zwischen Unternehmen und damit ein **neues Vertrags(-klausel)recht** im B2B-Bereich für die Datennutzung geschaffen wird. Dabei wäre es aber zu kurz gegriffen, würde man hierin eine reine Ergänzung zum nationalen AGB-Recht im Sinne der §§ 305 ff. BGB sehen. So ist im Sinne des Data Act irrelevant, ob es sich formal um allgemeine Geschäftsbedingungen handelt, das heißt insbesondere um für eine Vielzahl von Verträgen vorformulierte Vertragsbedingungen (§ 305 Abs. 1 S. 1 BGB), oder um einzelne Individualverträge. Weitere Vertragsklauseln enthält Art. 25 Data Act, was den Wechsel von Datenverarbeitungsdiensten vereinfachen soll.

3.1.4 Data Act und Urheberrecht / Geistiges Eigentum

Das **Urheberrecht sowie der Schutz des Rechts des geistigen Eigentums**[9] bleiben vom Data Act unberührt, Art. 1 Abs. 8 und ErwG. 13. Soweit also urheberrechtlich geschützte Werke von einer Datenweitergabe betroffen sind, kann darin eine Werknutzung liegen, die urheberrechtlich gerechtfertigt werden muss. Wenn allerdings Daten betroffen sind, die durch ein vernetztes Produkt oder einen verbundenen Dienst erlangt bzw. erzeugt wurden, greift der Schutz durch Art. 7 der Richtlinie über den rechtlichen Schutz von Datenbanken (RL 96/9/EG) bzw. das in Deutschland nach den §§ 87a ff. UrhG festgelegte Schutzrecht nicht – hier gilt der Anwendungsbereich des Data Act, Art. 43 Data Act.

Beispiel: Datenbereitstellung und Urheberrecht

Der Fahrzeughersteller Auto AG erhebt diverse Fahrzeugdaten in seinen Systemen in einer nach bestimmten Kriterien strukturierten Form, sodass die Daten möglichst nützlich etwa für Funktionalitätserweiterungen auf Seiten der Auto AG sind. Verlangt ein Nutzer rechtmäßig die in seinem Fahrzeug generierten Daten gemäß Art. 3 Abs. 1 Data Act heraus, so kann sich die Auto AG nicht als Gegenrecht darauf berufen, dass ihre Datensammlung urheberrechtlich eine Datenbank und damit gemäß § 87a Abs. 1 UrhG geschützt ist und die Auto AG allein gemäß § 87b Abs. 1 S. 1 UrhG bestimmen darf, wem sie Teile hiervon zugänglich macht. Der Anspruch gemäß Art. 3 Abs. 1 Data Act geht gemäß Art. 43 Data Act insoweit vor.

[9] Insbesondere RL 2001/29/EG, RL 2004/48/EG und RL (EU) 2019/790.

3.1.5 Data Act und Kriminalitätsbekämpfung

Schließlich berührt der Data Act nicht die Rechtsakte der Union und die nationalen Rechtsakte über die Datenweitergabe, den Datenzugang und die Datennutzung zum Zwecke der **Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten** oder der Strafvollstreckung, oder für Zoll- und Steuerzwecke[10], siehe Art. 1 Abs. 6 UAbs. 2 Satz 1 Data Act.

Auf weitere Querbeziehungen des Data Act soll hier nicht weiter eingegangen werden.[11]

3.1.6 Data Act und KI-Verordnung

Letztlich flankiert der Data Act ebenfalls die am 1. August 2024 in Kraft getretene Verordnung (EU) 2024/1689, kurz: **Verordnung über Künstliche Intelligenz (KI-VO)**. Diese und der Data Act stehen grundsätzlich nebeneinander. Das bedeutet: Je nachdem, ob es „nur“ um vernetzte Produkte bzw. KI-Anwendungen oder auch beides geht, finden entweder nur der Data Act bzw. die KI-Verordnung oder auch beide Anwendung. Wenn im Einzelfall tatsächlich einmal sowohl der Data Act als auch die KI-Verordnung zu beachten sind, müssen Unternehmen auch beide Regelwerke beachten und insbesondere die damit verbundenen Pflichten erfüllen. Die wesentlichen Pflichten aus dem Data Act sind in dem vorliegenden Leitfaden beschrieben. Die Pflichten, die auf bestimmte Unternehmen aus der KI-Verordnung zukommen, behandelt der nachstehende Exkurs. Soweit es sich dabei um Transparenz- und Informationspflichten handelt, lässt sich der zusätzliche Aufwand in Grenzen halten: Es geht jeweils darum, das Produkt oder den Dienst sowie die diesen zugrundeliegende KI-Anwendung so zu beschreiben, dass die Nutzer bzw. Betroffenen eine ausreichende Vorstellung von der Datenverarbeitung haben. Solche Dokumentationen werden Unternehmen schon aus eigenem Interesse erstellen, um die jeweilige Datenverarbeitung zielführend zu organisieren. Ähnlich wie man dies bereits von den Verarbeitungsverzeichnissen nach der Datenschutzgrundverordnung kennt, mag der eine dies als nervige Bürokratie, der andere als nützliche Unterstützung der Organisation eines datengetriebenen Geschäftsmodells empfinden.

Praxishinweis

Die zuständigen Behörden, insbesondere die Datenschutzaufsichtsbehörden, geben hilfreiche Informationen zum Datenrecht für Unternehmen. So gab das Bayerische Landesamt für Datenschutzaufsicht in einer Pressmitteilung vom 09. August 2024 die Errichtung eines neuen Themenschwerpunktes zu KI & Datenschutz bekannt. Dieser ist unter https://www.lda.bayern.de/de/ki.html abrufbar. Empfehlenswert ist auch ein Blick in das Informationsangebot der TU München unter www.baywidi.de.

[10] Hierzu gehört insbesondere die VO (EU) 2021/784, VO (EU) 2022/2065 und die VO (EU) 2023/1543 sowie die RL (EU) 2023/1543.
[11] Zum Beispiel wir die RL (EU) 2019/882 zur Festlegung von Barrierefreiheitsanforderungen durch den Data Act ergänzt, ErwG. 12.

Praxisbeispiele

Eine „Querbeziehung“ zwischen Data Act und KI-Verordnung gibt es etwa in den folgenden Fällen:

- **KI-Training mit IoT-Daten**: Der Data Act zielt auf eine Nutzung der vor allem durch sog. Internet-of-Things-Geräte (IoT) generierten Daten ab. Diese Daten können besonders interessant für Dritte sein, die durch diese Art von Daten KI-Modelle trainieren möchten. So könnte etwa ein Start-Up die von einem Smart-Fridge erhobenen Daten (z. B. im Kühlschrank enthaltene Lebensmittel) nutzen, um eine KI-basierte App mit Rezeptvorschlägen zu erstellen. In diesem Fall könnte sich das Start-Up als Datenempfänger im Sinne des Data Acts über einen Datenlizenzvertrag Zugangsrechte einräumen lassen. Durch die vom Data Act vorgesehenen Datenzugangsmöglichkeiten könnten KI-basierte Technologien profitieren und neuen Aufwind erlangen. Gerade weil das sog. Webcrawling – die Suche nach öffentlich zugänglichen Daten aus dem Internet – zunehmend unter Aspekten des Datenschutzes und des Urheberschutzes kritisch gesehen wird, gewinnen Datenlizenzverträge künftig an Bedeutung. Der Data Act schafft den Regulierungsrahmen dafür, dass Daten aus vernetzten Produkten und Anwendungen rechtskonform erlangt werden können. Sie stehen dann wiederum auch für das KI-Training zur Verfügung. Dies schafft einen Mehrwert, der letztlich auch wieder den Verbrauchern und weiteren Nutzern digitaler Produkte zugutekommt.

- **IoT-Gerät nutzt selbst KI**: Umgekehrt dürfte es nicht wenige vernetzte Geräte geben, die ihrerseits Funktionen besitzen, die auf KI-Anwendungen zurückgreifen. So beruht die Sprachsteuerung eines Smart Home Gerätes wie Alexa auf dem Training mit Sprachdaten. Der Anbieter solcher Smart Home Geräte muss deshalb die KI-Verordnung für ein rechtskonformes KI-Training genauso einhalten wie den Data Act, wenn es um Ansprüche auf Herausgabe der IoT-Daten geht.

Bislang wurden solche Geräte allein nach der DSGVO beurteilt. Nunmehr ergänzen der Data Act und die KI-Verordnung diese Regulierung. Dies kann im Einzelfall zu offenen Fragen führen, weil diese Regelwerke nicht optimal aufeinander abgestimmt sind. Eine daraus resultierende Rechtsunsicherheit muss aber nicht zu Lasten der Unternehmen gehen. Auch für die (Aufsichts-) Behörden ist diese Materie Neuland. Sie tasten sich an diese komplexe Rechtslage ebenso heran wie die Unternehmen selbst. Man muss deshalb auch keine Nachteile oder Sanktionen befürchten, solange man diese Gesetze nicht vollständig ignoriert und die auch im vorliegenden Leitfaden beschriebenen Basispflichten beachtet. Bis zur Geltung des Data Act ab dem 12.09.2025 und der KI-Verordnung (größtenteils ab dem 02. August 2026) wird es weitere hilfreiche Hinweise sowie Empfehlungen aus den Behörden, der Rechtspraxis und der Wissenschaft geben. So plant etwa das TUM Center for Digital Public Services eine interaktive Wissenslandkarte zu den EU-Rechtsakten, die insbesondere deren Rechtsbeziehungen untereinander illustrieren wird. Näheres hierzu ab 2025 unter www.tum-cdps.de.

3.1.7 Exkurs: Überblick über die KI-Verordnung

Der Einsatz von KI, insbesondere generativer KI (Textgeneratoren wie ChatGPT, aber auch andere Tools) in Unternehmen bietet **zahlreiche Vorteile**. Diese innovative Technologie revolutioniert nicht nur Arbeitsabläufe, sondern steigert auch die Effizienz und Kreativität. Durch maschinelles Lernen kann generative KI komplexe Aufgaben wie das Verfassen von Texten, das Entwerfen von Grafiken oder das Erstellen von Code übernehmen, wodurch menschliche Ressourcen für anspruchsvollere Aufgaben freigesetzt werden. Trotz großer Sorgen von Arbeitnehmern hinsichtlich ihrer beruflichen Zukunft: Generative KI wird sich weniger auf gesamte Berufe auswirken, jedoch stark auf konkret zu erledigende Aufgaben. Hier liegt das große Potential für Unternehmen.

Insgesamt bietet der Einsatz generativer KI Unternehmen die Möglichkeit, ihre **Innovationskraft** zu stärken und ihre **Wettbewerbsfähigkeit** in einer zunehmend digitalisierten Welt zu festigen. Die Einsatzfelder generativer KI im Unternehmen sind zahlreich.

Beispiele: Anwendungsfelder von KI in Unternehmen

- Verfassen von Dokumenten
- Datenanalyse
- Informationsbeschaffung
- Optimierung von Marketing- und Verkaufsaktivitäten
- Automatisierung wiederkehrender Aufgaben

Die KI-Verordnung will einerseits den **Schutz der Bürgerrechte und -sicherheit** gewährleisten und andererseits **Innovationskraft und Vertrauen in KI** fördern. Die Verordnung zielt darauf ab, einen rechtlichen Rahmen zu schaffen, der sowohl Risiken minimiert als auch das Potenzial der KI voll ausschöpft. Für Unternehmen ist die KI-Verordnung von zentraler Bedeutung, weil sie die Art und Weise regelt, wie KI-Systeme entwickelt, bereitgestellt und verwendet werden dürfen. Unternehmen, die KI-Lösungen entwickeln oder einsetzen, müssen sicherstellen, dass ihre Systeme den neuen rechtlichen Anforderungen entsprechen. Eine **Nichteinhaltung** kann **schwerwiegende finanzielle und rechtliche Konsequenzen** nach sich ziehen. Verstöße gegen die KI-Verordnung können mit erheblichen Bußgeldern geahndet werden – bis zu 6 % des weltweiten Jahresumsatzes eines Unternehmens oder 30 Millionen Euro, je nachdem, welcher Betrag höher ist. Daher ist es für Unternehmen unerlässlich, sich frühzeitig mit den neuen Regelungen auseinanderzusetzen und ihre KI-Systeme entsprechend anzupassen.

Die KI-Verordnung verfolgt einen **risikobasierten Ansatz**. Sie klassifiziert KI-Systeme nach ihrem Risiko für die Gesellschaft und Individuen in vier Kategorien: verbotene KI, Hochrisiko-KI, KI mit geringem Risiko und KI mit minimalem Risiko. Dies bedeutet, dass die Anforderungen an Unternehmen je nach Risikostufe der eingesetzten KI variieren.

Hochrisiko-KI: Hochrisiko-KI-Systeme sind solche, die in sensiblen Bereichen eingesetzt werden, wo sie erhebliche Auswirkungen auf das Leben von Menschen haben können. Beispiele sind KI-Systeme, die in der kritischen Infrastruktur (z. B. im Gesundheitswesen, in der Energieversorgung), bei der Bewertung von Kreditwürdigkeit oder in der Strafverfolgung eingesetzt werden. Unternehmen, die Hochrisiko-KI verwenden oder entwickeln, müssen besonders strenge Anforderungen erfüllen:

- **Vorherige Konformitätsbewertung:** Bevor ein Hochrisiko-KI-System in Betrieb genommen werden darf, muss es einer Konformitätsbewertung unterzogen werden. Diese Bewertung prüft, ob das System den in der Verordnung festgelegten Anforderungen entspricht.
- **Strengere Dokumentationspflichten:** Neben der allgemeinen Dokumentationspflicht müssen für Hochrisiko-KI-Systeme umfassendere technische Informationen bereitgestellt werden, die unter anderem die Algorithmen, Trainingsmethoden und Datenquellen beschreiben.
- **Regelmäßige Audits:** Hochrisiko-KI-Systeme müssen kontinuierlich überwacht und regelmäßig auf ihre Konformität überprüft werden. Dies kann auch externe Audits umfassen, die durch unabhängige Stellen durchgeführt werden.
- **Technische Sicherheitsanforderungen:** Hochrisiko-KI-Systeme müssen besonders robust und sicher gestaltet sein, um Missbrauch und Fehlfunktionen zu verhindern. Dazu gehört auch, dass Sicherheitslücken schnell behoben und Schwachstellen proaktiv identifiziert werden.

KI mit geringem Risiko: Für KI-Systeme, die als weniger risikoreich eingestuft werden, gelten weniger strenge Anforderungen. Dennoch müssen auch hier grundlegende Vorschriften eingehalten werden, wie etwa die **Transparenzpflicht und die Sicherstellung der Datenqualität**. Unternehmen, die solche KI-Systeme verwenden, sind nicht verpflichtet, Konformitätsbewertungen durchzuführen oder externe Audits zu veranlassen, sollten aber dennoch Maßnahmen ergreifen, um die Einhaltung der allgemeinen Vorschriften der Verordnung zu gewährleisten.

Unternehmen, die KI-Tools einsetzen möchten, müssen ungeachtet der Risikoeinstufung eine Reihe von Anforderungen erfüllen, um die Konformität mit der KI-Verordnung sicherzustellen. Diese Anforderungen hängen von der Risikostufe der eingesetzten KI ab, wobei der Schwerpunkt auf Hochrisiko-Anwendungen liegt.

Allgemeine Anforderungen:

- **Transparenzpflichten:** Unternehmen müssen sicherstellen, dass die Benutzer von KI-Systemen über die Funktionsweise und die potenziellen Risiken informiert sind. Dies betrifft insbesondere Systeme, die menschliche Interaktionen nachahmen, wie etwa Chatbots. Es muss klar kommuniziert werden, dass ein KI-System eingesetzt wird.
- **Dokumentation und Aufzeichnungen:** Unternehmen sind verpflichtet, eine umfassende Dokumentation ihrer KI-Systeme zu führen, die sowohl technische als auch organisatorische Maßnahmen beschreibt. Diese Dokumentation soll der Aufsichtsbehörde zur Verfügung gestellt werden können, um die Einhaltung der KI-Verordnung nachzuweisen.
- **Datenqualität und -sicherheit:** Die Qualität und Sicherheit der von der KI genutzten Daten ist ein zentraler Aspekt der Verordnung. Unternehmen müssen sicherstellen, dass

die Trainingsdaten ihrer KI-Systeme repräsentativ und frei von Verzerrungen sind, um faire und zuverlässige Entscheidungen zu ermöglichen. Zudem müssen Maßnahmen zur Datensicherheit und zum Schutz vor Cyberangriffen implementiert werden.
- **Monitoring und Risikoüberwachung:** Unternehmen müssen ihre KI-Systeme kontinuierlich überwachen, um sicherzustellen, dass sie ordnungsgemäß funktionieren und keine unvorhergesehenen Risiken entstehen. Dazu gehört auch die Einrichtung von Mechanismen, um mögliche Fehlfunktionen oder Sicherheitsrisiken frühzeitig zu erkennen und zu beheben.
- **Menschliche Aufsicht:** KI-Systeme, insbesondere solche in Hochrisikobereichen, müssen so gestaltet sein, dass Menschen die Kontrolle behalten. Dies kann durch menschliche Aufsicht oder Eingriffsmöglichkeiten sichergestellt werden.

3.2 Umsetzung der Datenregulierungsakte in Deutschland

Die Umsetzung der Datenregulierungsakte in Deutschland ist nach wie vor ein aktuelles Thema, mit dem sich etwa der Digitalausschuss des Deutschen Bundestages am 26. Juni 2024 befasst hat. Das zunächst restriktive Datenschutzrecht hat sich inzwischen zu einem **Datenwirtschaftsrecht** entwickelt, was Deutschland vor einige Herausforderungen in der Umsetzung stellt. So stellte sich im Digitalausschuss insbesondere die Frage, wie eine sichere, aber zugleich innovative Datenpolitik sichergestellt werden kann.

Praxishinweis: Nationale Gestaltungsspielräume beim Data Act?

Gerade im Hinblick auf die europäischen Datenräume ist problematisch, welche Entscheidungs- und Gestaltungsspielräume der deutsche Gesetzgeber hat. Explizite **Öffnungsklauseln** sieht der Data Act nicht vor. Lediglich in ErwG. 52 Data Act ist genannt, dass Mitgliedstaaten Vorgaben zum Zertifizierungsverfahren festlegen dürfen, einschließlich Aspekten zum Ablauf und Widerruf. Im Übrigen ist umstritten, inwieweit unionale Harmonisierungsvorschriften (wie solche des Data Acts) durch Mitgliedstaaten konkretisiert werden dürfen. Lediglich in den Bereichen, in den die EU keine oder nur eine eingeschränkte Gesetzgebungskompetenz besitzt (wie z. B. nationale Sicherheit) bestehen die üblichen Einschränkungsmöglichkeiten der Mitgliedstaaten. Insofern muss abgewartet werden, wie sich die Kommission gegenüber dem einen oder anderen nationalen Vorstoß verhält.

Was die **europäischen Datenräume** betrifft, dürfte dem nationalen Gesetzgeber insgesamt nur ein sehr begrenzter Konkretisierungsspielraum zukommen, wenn überhaupt. So geht aus ErwG. 103 Data Act hervor, dass weitere noch nicht vom Data Act geregelte Details zu Normung und Interoperabilität bei europäischen Datenräumen (vgl. Art. 33 Data Act) maßgeblich von der Kommission festgelegt bzw. deren Festlegung überwacht werden. Konkrete Anforderungen an die Festlegung gemeinsamer Spezifikationen finden sich in Art. 33 Data Act. Diese Vorschrift lässt dem nationalen Gesetzgeber allerdings keinen Spielraum. Vielmehr sieht Art. 33 Abs. 10 Data Act vor, dass ein Mitgliedstaat bei Zweifeln an der Konformität einer gemeinsamen Spezifikation mit den Vorgaben des Data Act sich an die

Kommission wenden muss, um sie darüber zu informieren. Selbst hat er sonst grundsätzlich keine Möglichkeit der Spezifizierung.

Sachverständige im Ausschuss sind sich uneinig, welche Ziele der Gesetzgeber dabei vorrangig erfüllen soll: Dies reichte von strikter Umsetzung des Datenschutzes über einheitliche Rechtsauslegung und -anwendung mit einer weniger zersplitterten Datenschutzaufsicht bis zu einem ausgewogenen Verhältnis von Datenschutz und Datenökonomie.[12]

Noch zu klären ist auch, wer **zuständige Aufsichtsbehörde** sein soll. Der Data Act sieht, wie auch die DSGVO, einen Durchsetzungsmechanismus vor. Dabei ist Deutschland als Mitgliedsstaat verpflichtet, eine oder mehrere zuständige Aufsichtsbehörden einzusetzen, die die Einhaltung der Regelungen des Data Acts überwachen, Art. 31 Abs. 1 Data Act. Diese Behörden sollen die im Data Act aufgelisteten Kompetenzen besitzen, wie bspw. ein Untersuchungsrecht, Bearbeitungen von Beschwerden übernehmen und Verstöße sanktionieren.

Bezüglich des Verhältnisses zu den bereits bestehenden Datenschutzaufsichtsbehörden sieht der Data Act selbst vor, dass diese Datenschutzaufsichtsbehörden nicht nur die Einhaltung der Regelungen aus der DSGVO, sondern auch die Einhaltung des Data Acts überwachen sollen, Art. 31 Abs. 2 lit. a Data Act. Dies lässt sich grundsätzlich als effizienzsteigernd werten, stellt Deutschland jedoch vor Herausforderungen in der Umsetzung. So sagt die Vorschrift insbesondere nichts über die originäre Zuständigkeit für die Einhaltung des Data Acts aus, sondern macht lediglich die Vorgabe, dass die Datenschutzbehörden bei ihrer originären Tätigkeit zugleich die Einhaltung des Data Acts überwachen. Sie müssen aber nicht die einzigen Stellen für diese Aufgabe sein.

In Deutschland bieten sich theoretisch mehrere Behörden an: Die Bundesnetzagentur, die bestehenden 18 Datenschutzbehörden, sektoral bestehende Behörden wie das Kraftfahrtbundesamt speziell für vernetzte Fahrzeuge oder das Bundesinstitut für Arzneimittel und Medizinprodukte für Hersteller von Medizinprodukten, sowie schließlich die Errichtung einer oder mehrerer vollständig neuer Behörden. Letztlich sollte allerdings sichergestellt werden, dass kein zu großes Netzwerk unterschiedlicher Behörden mit diversen Zuständigkeiten entsteht, denn dadurch würde eine einheitliche Überwachung des Data Acts und einheitliche Auslegung der Verordnung massiv erschwert werden.[13]

---

[12] Siehe https://www.bundestag.de/ausschuesse/a23_digitales/Anhoerungen/1006274-1006274.
[13] Vgl. bereits Gemeinsame Stellungnahme 2/2022 des EDSA und des EDSB zum Data Act, https://www.edpb.europa.eu/system/files/2023-03/edpb-edps_jointopinion_2022-02_data_act_proposal_de.pdf.

Der **Geltungsbeginn des Data Acts** erfolgt gestuft, wie Art. 50 Data Act zeigt.

- Der Data Act gilt ab dem 12.09.2025.
- Die Verpflichtung gemäß Artikel 3 Abs. 1 Data Act gilt für vernetzte Produkte und die mit ihnen verbundenen Dienste, die nach dem 12.09.2026 in Verkehr gebracht wurden.
- Kapitel III (Pflichten der Dateninhaber bei Weitergabe von Daten) gilt nur in Bezug auf Datenbereitstellungspflichten nach dem Unionsrecht oder nach im Einklang mit Unionsrecht erlassenen nationalen Rechtsvorschriften, die nach dem 12.09.2025 in Kraft treten.
- Kapitel IV (Missbräuchliche Vertragsklauseln in Bezug zu Datenzugang und Datennutzung zwischen Unternehmen) gilt für Verträge, die nach dem 12.09.2025 geschlossen wurden. Für Verträge, die am oder vor dem 12.09.2025 geschlossen wurden, sofern sie unbefristet sind oder ihre Geltungsdauer frühestens 10 Jahr nach dem 11.1.2024 endet, gilt Kapitel IV abweichend ab dem 12.09.2027.

4 Anwendungsbereich

Der Data Act in sachlicher, räumlicher und persönlicher Perspektive

4.1 Sachlicher Anwendungsbereich

Der Data Act reguliert den Zugang zu und Umgang mit Daten im Privatsektor.

Der **Begriff Daten** wird in Art. 2 Nr. 1 Data Act definiert als *jede digitale Darstellung von Handlungen, Tatsachen oder Informationen sowie jede Zusammenstellung solcher Handlungen, Tatsachen oder Informationen auch in Form von Ton-, Bild- oder audiovisuellem Material.*

Dabei erstreckt sich die Verordnung auf jegliche Daten, die von der Definition umfasst werden, das heißt sowohl auf personenbezogene als auch auf nicht-personenbezogene Daten. In Bezug auf personenbezogene Daten bezieht sich der Verordnungsgeber zur Einheitlichkeit auf die entsprechende Legaldefinition aus der DSGVO (Art. 2 Nr. 3 Data Act i.V.m. Art. 4 Nr. 1 DSGVO). Nicht-personenbezogene Daten werden negativ definiert als alle Daten, die keine personenbezogenen Daten sind (Art. 2 Nr. 4 Data Act).

Praxishinweis: Daten und Informationen

Art. 2 Nr. 1 Data Act verwendet den **Begriff der Information** als eine bestimmte (Darstellungs-) Form von Daten. Dies kann zunächst verwirren, weil Informationen herkömmlich definiert werden als das, was sich daraus ergibt, dass (Roh-) Daten in einen bestimmten Kontext bzw. Interpretationszusammenhang gestellt werden. Wenn eine solche Information wiederum in digitaler Form erfasst und damit maschinenlesbar wird, entstehen neue Daten, eben als digitale Darstellung der Information.

Der Gesetzgeber des Data Act hat die **Definition von „Daten“ aus dem Digital Governance Act** übernommen. Bereits dort findet sich in Kommentierungen berechtigte Kritik an der Begrifflichkeit, insbesondere im Hinblick auf den anderen Begriff der „Informationen“. Der Begriff des Datums im Rahmen des Data Acts sollte wohl abstrakt und losgelöst von anderen Verständnissen gelesen werden. Der Data Act schafft damit eher einen „neuen“ Begriff, der nicht mit dem Begriff des Datums im Rahmen der DSGVO vergleichbar ist.

Der Dateninhaber dürfte daher **nur dann Rohdaten weitergeben, wenn diese unmittelbar verständlich sind**. Sind sie dies nicht, so muss er sie vor Zugänglichmachung aggregieren. Dazu würde dann auch die Anforderung aus Art. 3 Abs. 1 Data Act passen, dass die Daten für den Nutzer einfach, in einem umfassenden, strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt werden müssen.

Schließlich spricht ErwG. 8 Data Act davon, dass eine Übermittlung von Rohdaten möglichst vermieden werden und Algorithmen für einen weitergehenden Erkenntnisgewinn möglichst am Ort der Datengenerierung eingesetzt werden sollen.

Vor diesem Hintergrund kann man vereinfacht sagen, dass Daten und Information im Data Act synonym gebraucht werden, die Bereitstellung und Herausgabe von Daten sich also nicht lediglich auf für Laien unverständliche Rohdaten, sondern auf aggregierte, aufbereitete Daten – eben: Informationen – bezieht.

Das alles bedeutet allerdings nicht, dass Geschäftsmodelle wie die zwischen Kfz-Herstellern Versicherungsunternehmen etwa bei Telematiktarifen obsolet wären. Die Kfz-Hersteller können sich weiterhin eine konkrete Aggregierung der telematikrelevanten Daten von den Versicherungsunternehmen bezahlen lassen, wenn dafür ein ganz bestimmtes Format oder eine spezielle Aufbereitung notwendig ist. Es dürfte gegenüber dem Nutzer ausreichen, wenn ein Nutzer die Sensordaten z. B. in einer Tabelle im PDF-Format ablesen kann. Versicherungsunternehmen brauchen die Daten vermutlich in einem anderen Format bzw. möchten die Daten direkt über eine spezielle Schnittstelle erhalten. Auch ist es denkbar, dass Versicherungsunternehmen die Daten in der Form der PDF-Tabelle auch deshalb nicht über den Umweg des Nutzers erhalten möchten, da hier möglicherweise ein Verfälschungsrisiko besteht. Dann dürfte der Anreiz vorhanden sein, die Daten unmittelbar zwischen Versicherer und Kfz-Hersteller zu übermitteln. Dazu könnten die Hersteller dann ein entsprechendes Entgelt verlangen

---

Ein wichtiger Teilbereich dieser Verordnung adressiert Daten, die durch **vernetzte Produkte** erzeugt und verarbeitet werden:

Ein vernetztes Produkt stellt einen Gegenstand dar, der Daten über seine Nutzung oder Umgebung erlangt, generiert oder erhebt und der Produktdaten über einen elektronischen Kommunikationsdienst, eine physische Verbindung oder einen geräteinternen Zugang übermitteln kann und dessen Hauptfunktion nicht die Speicherung, Verarbeitung oder Übertragung von Daten im Namen einer Partei – außer dem Nutzer – ist, Art. 2 Nr. 5 Data Act.

Praxishinweis

Auch wenn der Data Act durch die zunehmende Vernetzung von Produkten veranlasst ist und wesentliche Vorschriften sich gerade auf die Daten aus vernetzten Produkten beziehen, gilt dies nicht für die gesamte Verordnung. Das zeigt schon Art. 1 Abs. 2 Data Act: Danach gilt Kapitel II des Data Act für „Daten, …, die die Leistung, Nutzung und Umgebung von vernetzten Produkten und verbundenen Diensten betreffen“, während Kapitel V für „alle Daten des Privatsektors mit Schwerpunkt auf nicht-personenbezogenen Daten“ gilt. Das bedeutet, dass sich die zentralen Ansprüche auf Datenweitergabe von Unternehmen an Verbraucher und innerhalb von Unternehmen – und damit der wohl für Unternehmen wichtigste Pflichtenkreis des Data Acts – nur auf Daten aus vernetzten Produkten (bzw. verbundenen Diensten) beziehen, während die Datenherausgabe wegen einer Notlage

(„außergewöhnliche Notwendigkeit“) für alle (nicht-personenbezogene) Daten des Privatsektors gilt.

Ein Fahrzeug mit Sensoren und einer regelmäßigen Datenverbindung zum Hersteller, der die Daten etwa zur Produktoptimierung erhebt, stellt ein solches vernetztes Produkt dar. Eine Antenne, die den Datentransfer ermöglicht oder eine Festplatte, worauf die Daten gespeichert werden, gehört nicht dazu.

Die Verordnung erfasst auch virtuelle Assistenten, soweit diese mit einem vernetzten Produkt oder Dienst interagieren, Art. 1 Abs. 4 Data Act. Von dem Begriff des Produktes können Fahrzeuge, Schiffe, Flugzeuge, landwirtschaftliche oder Industriemaschinen, Smart-Home-Geräte (z. B. Saugroboter oder Smart-Fridges) sowie Konsumgüter, medizinische Geräte und Lifestyle-Geräte umfasst sein.

Beispiel Fahrzeug als vernetztes Produkt

Am Beispiel eines Fahrzeugs als vernetztem Produkt lässt sich illustrieren, welche Daten entstehen und vom Data Act erfasst werden.

Das Fahrzeug ist mit diversen Sensoren ausgestattet (z. B. Multifunktionskameras, Radar-, Ultraschall- und Lidarsensoren). Diese Sensoren lassen sich grob in zwei Kategorien aufteilen: interne Fahrzeugerfassung und externe Fahrzeugerfassung.[14]

- Zu den **internen Sensoren** zählen etwa Beschleunigungssensor, Pedalweggeber, Reifenluftdruckverlust-Sensor, Tankdrucksensor, Sitzbelegungssensor, Drehzahlsensor.
- Zu den **externen Sensoren** zählen etwa Frontkameras, Rückkameras, Radar-, Lidar- und Ultraschallsensoren, Notbremssensoren, Regensensor, Temperatursensoren.

Mittels dieser Sensoren erfasst das Fahrzeug regelmäßig Umgebungsdaten, Fahrzeugdaten, Fahrerdaten. Darüber hinaus werden auch sonstige drittanbieterbezogene Daten verarbeitet.

- Zu den **Umgebungsdaten** zählen z. B. Daten anderer Verkehrsteilnehmer, aus der Verkehrsinfrastruktur, aus Verkehrsereignissen.
- Zu den **Fahrzeugdaten** zählen z. B. Grunddaten des Fahrzeugs, Kfz-Betriebswerte, aggregierte Fahrzeugdaten, technische Daten.
- Zu den **Fahrerdaten** zählen z. B. Infotainment- und Komforteinstellungen, Standort- und Navigationsdaten, Daten zum Fahrverhalten, Daten vom Smartphone des Fahrers, Daten zum Tankverhalten.
- Zu den sonstigen **drittanbieterbezogenen Daten** gehören solche Daten die z. B. von Versicherungen, Navigationsdienstleistern und weiteren Akteuren erzeugt und verarbeitet werden.

---

[14] Vgl. auch Wiebe/Helmschrot/Kreutz, CR 2023, 484 ff.

Sind diese Daten über einen elektronischen Kommunikationsdienst wie eine mobile Datenverbindung oder auch über eine physische Schnittstelle auslesbar, so fallen sie in den Anwendungsbereich.

Diese Datenerhebungen dienen diversen Zwecken, wie etwa der Fahrsicherheit, dem Insassenschutz, Versicherungszwecken, Verbesserung der Verkehrseffizienz, Umweltschutz, Unterhaltungs- und Informationszwecken oder schlicht Marketingzwecken.[15]

Art. 2 Nr. 2 Data Act i.V.m. ErwG. 16 nimmt solche Produkte wieder vom Anwendungsbereich aus, die in erster Linie dazu bestimmt sind, Inhalte anzuzeigen oder abzuspielen oder diese – unter anderem für die Nutzung durch einen Online-Dienst – aufzuzeichnen und zu übertragen, da diese für separate Märkte von Text und audiovisuellen Inhalten relevant sind.

> ErwG. 16 lautet (hier im Auszug): Diese Verordnung ermöglicht es Nutzern vernetzter Produkte, … Dienste zu nutzen, die auf Daten basieren, die von in diese Produkte eingebetteten Sensoren erhoben werden, …. Es ist wichtig, einerseits die Märkte für die Bereitstellung solcher mit Sensoren ausgestatteter vernetzter Produkte und damit verbundener Dienste und andererseits die Märkte für … Text-, Audio- oder audiovisuelle Inhalte, die häufig Rechten des geistigen Eigentums unterliegen, voneinander abzugrenzen. Daher sollten Daten, die von solchen mit Sensoren ausgestatteten vernetzten Produkten generiert werden, wenn ihre Nutzer Inhalte – unter anderem zur Nutzung durch einen Online-Dienst – aufzeichnen, übermitteln, anzeigen lassen oder abspielen, sowie die Inhalte selbst, die häufig Rechten des geistigen Eigentums unterliegen, nicht unter diese Verordnung fallen.

ErwG. 16 Data Act zielt auf die Abgrenzung zwischen spezifisch für die Nutzung vernetzter Produkte programmierte Software und sonstige reguläre Software ab.

Beispiele: Allgemeine Software und Spezifische Software für vernetzte Produkte

---

- Solche **spezifische Software** wäre beispielsweise eine von einem E-Bike-Hersteller angebotene mobile Anwendung (App), bei deren Nutzung ein E-Bike erst seine volle Funktionalität entfaltet. Oder aber im Rahmen von Fahrzeugen wie bei Škoda die MyŠkoda-App, mit der etwa Beleuchtungsmodalitäten im Fahrzeug eingestellt werden können oder die Standheizung von unterwegs eingeschaltet und gesteuert werden kann. Gleichzeitig lassen sich ebenfalls Daten wie gefahrene Entfernungen oder weitere Daten auslesen.
- Wenn ein Nutzer demgegenüber eine **allgemeine, nicht spezifisch für das Produkt entwickelte App** nutzt, wie beispielsweise eine Tagebuch-/Journaling-App, die die GPS- und weitere Daten des Fahrzeugs ebenfalls auslesen bzw. übermitteln lassen kann und

---

[15] Wiebe/Helmschrot/Kreutz, CR 2023, 484, 485.

dem Nutzer so die Tagebucheinträge vorformuliert, sollen diese Daten dann nicht unter den Data Act fallen.

Grund für diese Unterscheidung ist – wie ErwG. 16 Data Act es hervorhebt – das Urheberrecht, das hier losgelöst von der Generierung von Internet-of-Things-Daten zur Geltung kommen soll. Wenn der Nutzer also die Journaling-App nutzt, die der Journaling-App-Anbieter über die App verarbeitet, wird dieser damit dann nicht zum Dateninhaber.

4.2 Räumlicher Anwendungsbereich

Art. 1 Abs. 3 Data Act regelt den räumlichen Anwendungsbereich, also die Frage, in welchen Gebietsgrenzen die Vorschriften greifen und was hierfür der Anknüpfungspunkt ist. Ähnlich wie bei der DSGVO stellt der Data Act auf das **Marktortprinzip** ab. Seine Regelungen betreffen damit nicht nur Unternehmen, die ihren Geschäftssitz in der Europäischen Union haben und dort ihre Produkte vertreiben. Vielmehr gelten diese auch für Hersteller vernetzter Produkte und Anbieter von verbundenen Diensten, Dateninhaber und Anbieter von Datenverarbeitungsdiensten, die gegebenenfalls außerhalb der Union – beispielsweise in den USA – ihre Niederlassung besitzen. Entscheidend ist in diesem Fall, dass ihre **Produkte bzw. Dienste in der EU in Verkehr gebracht bzw. genutzt** werden. Der Data Act soll somit dann gelten, wenn durch datenverarbeitende Produkte oder Dienste sowie Cloud-Dienste Nutzer in der EU betroffen sind.

Auf den Ort der Niederlassung kommt es letztlich nur insoweit an, als es um die Datenverarbeitung selbst geht, wenn also der der **Datenempfänger** eine **Niederlassung in der Union hat** und dort die Daten bereitgestellt werden. Auch bei den **öffentlichen Stellen**, die im Falle einer außergewöhnlichen Notwendigkeit die Bereitstellung von Daten von Dateninhabern verlangen, wird darauf abgestellt, ob der Behördensitz in der EU liegt.

4.3 Persönlicher Anwendungsbereich

Der Data Act regelt nicht nur, aber doch vorrangig den Privatsektor. Konkret erfasst sind zwei Konstellationen: Nach Art. 1 Abs. 3 Data Act gilt der Rechtsakt für **Hersteller vernetzter Produkte** (wie etwa die Auto AG als Herstellerin eines vernetzten Fahrzeugs), die ihre Produkte in der EU in Verkehr bringen, und **Anbieter verbundener Dienste**, die sie in der Union zur Verfügung stellen.

Nach Art. 2 Nr. 6 ist ein **verbundener Dienst** ein *digitaler Dienst und namentlich auch Software, der zum Zeitpunkt des Kaufs, der Miete oder des Leasings so mit dem Produkt verbunden ist, dass das vernetzte Produkt ohne ihn eine oder mehrere seiner Funktionen nicht ausführen könnte oder der anschließend vom Hersteller oder einem Dritten mit dem Produkt verbunden wird, um die Funktionen des vernetzten Produkts zu ergänzen, zu aktualisieren oder anzupassen, und bei dem es sich nicht um einen elektronischen Kommunikationsdienst handelt.*

Diese Definition umfasst etwa die **ergänzende Software eines Drittanbieters** in einem vernetzten Fahrzeug wie eine Technologie, die ergänzend heruntergeladen und installiert werden kann und speziell Verkehrsstörungen (z. B. Staus) oder besondere Verkehrssituationen (z. B. vereiste Fahrbahn) erkennt und zusammen mit anderen Fahrzeugen austauscht, die ebenfalls über diese Technologie verfügen.

Solche verbundenen Dienste können ebenso Software zur sonstigen Nutzung des vernetzten Fahrzeugs umfassen, womit etwa die Beleuchtung, die Lüftung oder auch Komfort-Funktionen wie die Medienwiedergabe bedient werden kann.

Beispiel: verbundener Dienst

Die Cockpit GmbH hat sich auf Software spezialisiert, die diverse Funktionen in einem Fahrzeug im digitalen Cockpit anzeigt und mit der man das digitale Cockpit aktiv steuern kann. So lassen sich etwa die Beleuchtung und die Fenster am Fahrzeug regulieren oder die Sensoren zum Drehmoment oder zur aktuellen Bremskraft überwachen. Sie bietet hierzu regelmäßige Updates und weitere für den Nutzer ergänzend buchbare Komfortfunktionen. Die Auto AG kooperiert mit der Cockpit GmbH und verbaut in ihren Fahrzeugen die Software der Cockpit GmbH. Die Cockpit GmbH ist insoweit Anbieterin eines verbundenen Dienstes. Es kommt nicht darauf an, ob es sich um eine notwendige Funktion handelt oder um eine Komfortfunktion, welche durch den verbundenen Dienst erbracht wird.

Darüber hinaus findet die Verordnung Anwendung auf sog. **Dateninhaber**.

Ein **Dateninhaber** ist nach Art. 2 Nr. 13 Data Act eine *natürliche oder juristische Person, die nach dieser Verordnung, nach geltendem Unionsrecht oder nach nationalen Rechtsvorschriften zur Umsetzung des Unionsrechts 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*.

Beispiel: Vom Softwareanbieter zum Dateninhaber

Die Cockpit GmbH hat ihre Software wie im Beispiel zuvor in die Fahrzeuge der Auto AG eingebaut. Zum Dateninhaber wird sie dann, wenn sie die Software nicht bloß in das Fahrzeug verbaut, sondern über diesen Einbau hinaus Fahrzeugdaten kontinuierlich erhebt. Damit wird sie von einem bloßen Softwareanbieter zu einem Dateninhaber.

Ferner normiert die Verordnung Rechte und Pflichten von Datenempfängern.

Datenempfänger werden nach Art. 2 Nr. 14 Data Act definiert als *natürliche oder juristische Personen, die zu Zwecken innerhalb ihrer gewerblichen, geschäftlichen, handwerklichen oder beruflichen Tätigkeit handeln, ohne Nutzer eines vernetzten Produktes oder verbundenen Dienstes zu sein, und denen vom Dateninhaber Daten bereitgestellt werden, einschließlich Dritter, denen der Dateninhaber auf Verlangen des Nutzers oder im Einklang mit einer rechtlichen Verpflichtung aus anderem Unionsrecht oder aus nationalen Rechtsvorschriften, die im Einklang mit Unionsrecht erlassen wurden, Daten bereitstellt.*

Diese zunächst komplex anmutende Definition versteht unter Datenempfängern Menschen oder Unternehmen, die Daten erhalten, um diese Daten beruflich für ihre eigenen Produkte zu nutzen.

Beispiel: Datenbereitstellung für Telematiktarif

Auf dem Fahrzeugmarkt bietet die Car Insurance KG Kfz-Versicherungsmodelle an, die anhand von Fahrdaten bestimmte individuelle Tarife ermöglichen. Bei diesen Tarifen wird die Höhe der Versicherungsbeiträge an die speziellen Fahrer- bzw. Fahreigenschaften geknüpft. Die Halterin und Nutzerin eines Fahrzeugs der Auto AG wünscht sich einen besonders günstigen, auf sie abgestimmten Versicherungstarif. Sie macht daher vom Angebot *Pay-as-you-drive-* bzw. *Pay-how-you-drive*-Tarif Gebrauch. Sie vereinbart mit den Parteien, dass die Auto AG der Car Insurance KG die entsprechenden Fahrer- und Fahrzeugdaten zugänglich macht und zum Abruf bereitgestellt. Die Car Insurance KG nimmt damit die Rolle der Datenempfängerin im Sinne des Data Acts ein.

Als weiterer Adressat benennt die Verordnung **Anbieter von Datenverarbeitungsdiensten**.

Ein **Datenverarbeitungsdienst** stellt eine *digitale Dienstleistung dar, die einem Kunden bereitgestellt wird und einen flächendeckenden und auf Abruf verfügbaren Netzzugang zu einem gemeinsam genutzten Pool konfigurierbarer, skalierbarer und elastischer Rechenressourcen zentralisierter, verteilter oder hochgradig verteilter Art ermöglicht, die mit minimalem Verwaltungsaufwand oder minimaler Interaktion des Diensteanbieters rasch bereitgestellt und freigegeben werden können*, Art. 2 Nr. 12 Data Act.

Beispiel Cloud-Dienst

Ein Kunde (wiederum eine natürliche Person oder ein Unternehmen) möchte häufig einen von überall und jederzeit nutzbaren Service nutzen, bei dem die Daten bspw. zentral in einer Cloud gespeichert bzw. verarbeitet werden. Dies kann etwa in Form eines Plattform-as-a-Service geschehen. Der Cloud-Dienstleister würde hier als Datenverarbeitungsdienst im Sinne des Data Acts fungieren.

Gemäß ErwG. 80 zählen zu den erwähnten **Rechenressourcen** etwa Netze, Server oder sonstige virtuelle oder physische Infrastrukturen, Software – einschließlich Tools zur Entwicklung von Software –, Speicher, Anwendungen und Dienste.

- Der Begriff **"ortsunabhängig"** wird verwendet, um zu beschreiben, dass die Bereitstellung der Rechenkapazitäten über das Netz und der Zugang zu ihnen über Mechanismen erfolgt, die den Einsatz heterogener Thin- oder Thick-Client-Plattformen (von Webbrowsern bis hin zu mobilen Geräten und Arbeitsplatzrechnern) fördern.
- Der Begriff **"skalierbar"** bezeichnet Rechenressourcen, die unabhängig von ihrem geografischen Standort vom Anbieter von Datenverarbeitungsdiensten flexibel zugewiesen werden, um Nachfrageschwankungen auszugleichen.
- Der Begriff **"elastisch"** dient zur Beschreibung der Rechenressourcen, die entsprechend der Nachfrage bereitgestellt und freigegeben werden, um je nach Arbeitsaufkommen zügig verfügbare Ressourcen auf bzw. abbauen zu können.
- Der Begriff **"gemeinsam genutzter Pool"** dient zur Beschreibung der Rechenressourcen, die mehreren Nutzern bereitgestellt werden, die über einen gemeinsamen Zugang auf den Dienst zugreifen, wobei die Verarbeitung jedoch für jeden Nutzer getrennt erfolgt, obwohl der Dienst über dieselbe elektronische Ausrüstung erbracht wird.
- Der Begriff **"verteilt"** dient zur Beschreibung der Rechenressourcen, die sich auf verschiedenen vernetzten Computern oder Geräten befinden und die untereinander durch Nachrichtenaustausch kommunizieren und sich koordinieren.
- Der Begriff **"hochgradig verteilt"** dient zur Beschreibung der Datenverarbeitungsdienste, bei denen Daten näher an dem Ort verarbeitet werden, an dem sie generiert oder erhoben werden, z. B. in einem vernetzten Datenverarbeitungsgerät. Edge-Computing, eine Form dieser hochgradig verteilten Datenverarbeitung, dürfte neue Geschäftsmodelle und Cloud-Dienste hervorbringen, die von Anfang an offen und interoperabel sein sollten.

Zu **Anbietern von Datenverarbeitungsdiensten** zählen insbesondere **Cloud-Anbieter**, die einen Pool von Daten zur Verfügung stellen. Auch hier soll ein Nutzer möglichst leicht einen solchen Anbieter wechseln können. Im Rahmen von personenbezogenen Daten gewährt die DSGVO bereits heute ein vergleichbares – obgleich bislang eher selten genutztes – Recht auf Datenübertragbarkeit, Art. 20 DSGVO.

Beispiel: Datenbereitstellung für Datenverarbeitungsdienst

Die Halterin eines Fahrzeugs der Auto AG nutzt einen Service der Wolke oHG. Dieser Service speichert Daten über ihre letzten Fahrten und wertet sie grafisch etwa im Hinblick auf Strecke, Kraftstoffverbrauch etc. aus. Auf diesen Service kann die Halterin jederzeit und von jedem Ort aus zugreifen, in dem sie sich über ein Portal bei ihrem Konto bei der Wolke oHG anmeldet.

5 Rechte und Pflichten für Unternehmen

Regulierung von Datenbereitstellung und Datennutzung

5.1 Bereitstellung von Produkt- und Dienstleistungsdaten für den Nutzer

Kapitel II, also die Art. 3 bis 7 Data Act gehören zu den wichtigsten Abschnitten des Data Acts. Aus ihnen ergeben sich verbindliche Unternehmenspflichten und korrespondierende Rechte der Nutzer. Nach Art. 7 Abs. 2 Data Act sind „Vertragsklauseln, die zum Nachteil des Nutzers die Anwendung der Rechte des Nutzers nach diesem Kapitel ausschließen, davon abweichen oder die Wirkung dieser Rechte abändern, … für den Nutzer nicht bindend." Dieses **Benachteiligungsverbot** lehnt sich an das europäische Verbraucherschutzrecht an.

5.1.1 Informationspflichten bei vernetzten Produkten, Art. 3 Data Act

Art. 3 Data Act begründet eine neue Pflicht für Unternehmen, die vernetzte Produkte herstellen oder verbundene Dienste anbieten. Sie müssen die damit verbundenen Produktdaten und Dienstdaten für den Nutzer zugänglich machen.

Dies muss für den Nutzer
- einfach (also leicht verständlich und ohne Umwege)
- sicher (also ohne Nachteile beim Zugriff auf diese Informationen)
- unentgeltlich (also ohne Kosten)
- in einem umfassenden, strukturierten, gängigen und maschinenlesbaren Format
- und direkt zugänglich (soweit technisch durchführbar)

geschehen.

Der Begriff des **maschinenlesbaren Formats** wird nicht näher definiert. Das Amt für Veröffentlichungen der Europäischen Union versteht den Begriff der Maschinenlesbarkeit[16] etwa dahingehend, dass Maschinen „Rechtstexte automatisch extrahieren, umformen und verarbeiten" können.[17]

Mit der direkten Zugänglichkeit ist das Prinzip **„Data Extraction by Design"** angesprochen. Damit ist gemeint, dass ein IT-System so konzipiert wird, dass jene Daten, die von einem Nutzer beansprucht werden können, nicht erst auf dessen Verlangen herausgegeben werden, sondern er dies grundsätzlich selbst über eine passende Schnittstelle tun kann. Dies setzt natürlich voraus, dass dies für das Unternehmen technisch durchführbar ist, was man im Einzelfall bewerten muss.

---

[16] Im deutschen Recht kennt man den Begriff aus § 12 EGovG: „Stellen Behörden über öffentlich zugängliche Netze Daten zur Verfügung, an denen ein Nutzungsinteresse, insbesondere ein Weiterverwendungsinteresse im Sinne des Datennutzungsgesetzes, zu erwarten ist, so sind grundsätzlich maschinenlesbare Formate zu verwenden."
[17] https://eur-lex.europa.eu/eli-register/news_item_7.html?locale=de.

Weiter müssen nach Art. 3 Abs. 2 Data Act **Anbieter vernetzter Produkte** vor dem Abschluss eines Kauf-, Miet- oder Leasingvertrags dem Nutzer Informationen über die Art, das Format und den Umfang der Produktdaten, die Fähigkeit zur Echtzeitdatengenerierung, Speichermöglichkeiten und den Zugang zu diesen Daten bereitstellen.

Nach Art. 3 Abs. 3 Data Act müssen wiederum **Anbieter verbundener Dienste** Nutzern Informationen über die Datenerhebung, die Speicherung und die Nutzung der Daten, die Identität des Dateninhabers, mögliche Kommunikationsmittel, Weitergabeoptionen, Beschwerderechte und etwaige Geschäftsgeheimnisse bereitstellen, sowie die Vertragsdauer und Kündigungsbedingungen klären.

Die Informationen sollen gemäß ErwG. 24 über eine Webseite oder einen QR-Code **auf einfache Weise bereitgestellt** werden können. Geschieht dies nicht, sind die Daten gem. Art. 4 Data Act dem Nutzer vom Dateninhaber direkt und in Echtzeit zur Verfügung zu stellen und – falls möglich – auch auf elektronischem Wege.

Beispiel: Datenbereitstellung für Fahrzeugservices

Ein Kunde erwirbt ein Fahrzeug der Auto AG. Dieses Fahrzeug bietet verschiedene Funktionen. Dazu gehören Sensoren für das Halten der Spur sowie die des Abstands zum vorausfahrenden Fahrzeug (Travel Assist) und für die Überwachung der Flüssigkeiten wie Öl und Wischwasser. Zusätzlich werden Daten zur Einstellung des Fahrersitzes und der Lieblingstemperatur erhoben. Diese Daten werden über eine „Always-On-Demand“-Schnittstelle in regelmäßigen Abständen über ein Mobilfunknetz an die Auto AG übertragen. Die Daten nutzt die Auto AG zur Ermittlung des Fahrsicherheitsniveaus, der Langlebigkeit des Fahrzeugs bzw. des Ausbaus von weiteren Komfortfunktionen. Vor Abschluss des Kaufvertrags über das Fahrzeug muss die Auto AG dem Kunden Informationen über diese Daten mitteilen, mindestens das Daten-Format (bspw. CSV- oder PDF-Format) inklusive Umfang der Daten, ob das Fahrzeug die Daten in Echtzeit generiert, ob und ggf. wie lange sie extern gespeichert werden, sowie auf welche Art und Weise der Nutzer auf die Daten zugreifen kann, bspw. indem der Nutzer die Daten in einer Partnerwerkstatt auslesen und sich auf einem Speichermedium in Tabellenform herausgeben lassen kann. Denkbar ist hier auch, dass die Auto AG etwa eine Plattform betreibt, in die sie die o.g. Daten einpflegt, so dass ihre Kunden direkt darauf zugreifen können. Die Investition hierfür könnte sich langfristig durch ersparte Transaktionskosten amortisieren.

5.1.2 Datenzugang für Nutzer vernetzter Produkte, Art. 4 Data Act

Art. 4 Data Act regelt die Rechte und Pflichten von Nutzern und Dateninhabern in Bezug auf den Zugang zu sowie die Nutzung und die Bereitstellung von Produktdaten und verbundenen Dienstdaten.

Soweit der Nutzer nicht direkt vom vernetzten Produkt oder verbundenen Dienst aus auf die Daten zugreifen kann, stellen die Dateninhaber nach Art. 4 Abs. 1 Data Act dem Nutzer ohne Weiteres verfügbare Daten einschließlich der zur Auslegung und Nutzung der Daten erforderlichen Metadaten bereit, und zwar ähnlich wie bei Art. 3 Data Act (siehe 5.1.1):

- unverzüglich
- einfach
- sicher
- unentgeltlich
- in einem umfassenden, gängigen und maschinenlesbaren Format
- in der gleichen Qualität wie für den Dateninhaber
- kontinuierlich
- in Echtzeit

Dies geschieht auf einfaches Verlangen auf elektronischem Wege, soweit dies technisch durchführbar ist. Den Maßstab hierfür bestimmt der Data Act. Dieser kann sich aus Branchenstandards ergeben, die sich möglicherweise auch erst etablieren müssen.

Zu den verfügbaren Daten gehören zunächst einmal die **generierten Rohdaten**, die entweder unmittelbar von der jeweiligen Maschine produziert oder sensorgestützt erhoben werden oder durch tiefen-integrierte bzw. eingebettete Anwendungen aufgezeichnet wurden, einschließlich Anwendungen, die den Hardwarestatus und Funktionsstörungen angeben.[18]

Zu diesen **Daten** gehören darüber hinaus auch solche, die von dem **vernetzten Produkt oder verbundenen Dienst generiert** werden, während der Nutzer inaktiv ist, etwa wenn er beschließt, ein vernetztes Produkt für einen bestimmten Zeitraum nicht zu verwenden, sondern es im Bereitschaftszustand zu belassen oder sogar auszuschalten, da sich der Status eines vernetzten Produkts oder seiner Komponenten, beispielsweise seiner Batterien, ändern kann, wenn sich das vernetzte Produkt im Bereitschaftszustand befindet oder ausgeschaltet ist.[19] Dazu gehören Daten, die von einem einzelnen Sensor oder einer Gruppe miteinander verbundener Sensoren erhoben wurden, um die erfassten Daten für vielfältige Anwendungsfälle verständlich zu machen, indem eine physikalische Größe oder Eigenschaft oder die Veränderung einer physikalischen Größe, wie Temperatur, Druck, Durchflussmenge, Ton, pH-Wert, Flüssigkeitsstand, Position, Beschleunigung oder Geschwindigkeit, bestimmt wird.[20]

Vom **Zugangsanspruch** umfasst sind allerdings lediglich die generierten Daten an sich **(Rohdaten)** und gerade nicht daraus vom Dateninhaber abgeleitete Folgerungen. Aus den generierten Daten gefolgerte oder abgeleitete Informationen, die das Ergebnis zusätzlicher Investitionen in die Zuweisung von Werten oder Erkenntnissen aus den Daten sind (insbesondere mittels komplexer fremder Algorithmen, einschließlich solcher, die Teil weiterer

[18] ErwG. 15 Data Act.
[19] ErwG. 15 S. 8 Data Act.
[20] ErwG. 15 S. 9 Data Act.

Softwarekomponenten sind), fallen nicht in den Anwendungsbereich des Data Acts.[21] Dateninhaber sind bezogen auf diese Daten **nicht verpflichtet, ihre veredelten Daten einem Nutzer oder Datenempfänger bereitzustellen**. Der Data Act zielt nämlich nicht auf eine generelle Vergemeinschaftung von Daten und Informationen und damit verbundenen Investitionen ab, sondern etabliert lediglich einen Zugang zu den originär durch die Nutzung des Produktes oder Dienstes entstandenen Daten, die gewissermaßen in die Sphäre des Nutzenden fallen.

Beispiel: Herausgabe von Fahrzeugdaten

Der Fahrer eines käuflich erworbenen vernetzten Fahrzeugs, das von der Auto AG hergestellt wurde, generiert mit der Nutzung seines Fahrzeugs eine Vielzahl von Daten wie u. a. Daten zum Ölstand, gemessen in Litern pro gefahrenem Kilometer. Diese Daten könnte der Nutzer herausverlangen. Sofern die Auto AG mit diesen Daten weitere Analysen durchführt, mittels eigens erstelltem Berechnungsalgorithmus eine Effizienzkalkulation erstellt, oder sie z. B. für dieses Modell in eine statistische Relation mit Vorgängermodellen setzt, Schlussfolgerungen für die Produktion der kommenden Modellreihe zu ziehen, kann der Nutzer Zugang zu diesen weiteren Berechnungen und Informationen nicht verlangen.

Dabei trifft den Hersteller zunächst gemäß Art. 3 Data Act die Pflicht, das vernetzte Produkt von Grund auf so herzustellen, dass die vom Produkt oder verbundenem Dienst erzeugten Daten **grundsätzlich für den Nutzer direkt zugänglich** sind, etwa auf dem Gerät selbst oder in der Cloud (siehe bereits oben 5.1.1 zum Prinzip „Data Extraction by Design). Technisch sind unterschiedliche Lösungen denkbar, die sich nach Inkrafttreten des Data Acts erst entwickeln müssen, dies nicht zuletzt im Wettbewerb der Hersteller, die damit auch werben können. Der Data Act macht hier kaum Vorgaben. Vielleicht setzt sich auch eine besonders nutzerfreundliche Lösung durch, bei der die Daten je nach Produkt direkt dort (etwa in einem Fahrzeug) oder von dort aus (in einer Cloud) gespeichert und zum Abruf bereitgestellt werden. Dies wäre besonders für solche Konstellationen interessant, bei denen personenbeziehbare Daten auf diese Weise dezentral verbleiben und erst beim Hersteller für weitere Analysen anonymisiert weiterverarbeitet werden. Insgesamt muss den Herstellern vernetzter Produkte hier auch ein Gestaltungsspielraum zugestanden werden, weil ihre berechtigten und auch grundrechtlich geschützten wirtschaftlichen Interessen mit den Nutzerinteressen abgewogen werden müssen.

Gemäß Art. 4 Abs. 2 Data Act können Nutzer und Dateninhaber den **Datenzugang und die -nutzung vertraglich beschränken**, soweit Sicherheitsanforderungen betroffen sind.

Art. 4 Abs. 2 Data Act ist als **Ausnahmevorschrift** mit den besonderen Merkmalen der „Sicherheitsanforderungen“ und damit verbundenen „schwerwiegenden nachteiligen Auswirkungen auf die Gesundheit oder die Sicherheit von natürlichen Personen“ **sehr eng**

[21] ErwG. 15 S. 11 Data Act.

auszulegen. Der Grundgedanke hinter dieser Norm dürfte vergleichbar mit der Grundintention des Cyber Resilience Acts (CRA) sein. So heißt es z. B. in ErwG. 58 S. 1, 2 CRA: „*In bestimmten Fällen kann ein Produkt mit digitalen Elementen, das dieser Verordnung entspricht, dennoch ein erhebliches Cybersicherheitsrisiko oder ein Risiko für die Gesundheit oder Sicherheit von Personen, für die Erfüllung der Pflichten aus dem Unionsrecht oder dem nationalen Recht zum Schutz der Grundrechte, für die Verfügbarkeit, Integrität oder Vertraulichkeit von Diensten, die über ein elektronisches Informationssystem von wesentlichen Einrichtungen der in [Anhang I der Richtlinie … genannten Art angeboten werden, oder für andere Aspekte des Schutzes öffentlicher Interessen darstellen. Daher müssen Vorschriften festgelegt werden, die die Minderung solcher Risiken gewährleisten*.“ Die Einschränkung der Nutzung von Daten im Sinne von Art. 4 Abs. 2 Data Act könnte eine solche **Risikominderungsmaßnahme** sein.

Beispiele für Datenzugangsbeschränkung aus Sicherheitsgründen

- So fallen solche Szenarien unter Art. 4 Abs. 2 Data Act, wo durch die Nutzung des vernetzten Fahrzeugs auch Daten über die Nutzung der Datenschnittstellen (APIs) und der dahinterliegenden technischen Infrastruktur erzeugt werden. Diese könnten aus Gründen der Erhaltung der Cyberresilienz so sensibel sein, dass diese Daten nicht dem Nutzer bereitgestellt werden, sodass keinerlei Informationen über diese sicherheitsrelevanten Schnittstelle nach außen dringen (z. B. Ineinandergreifen bestimmter technischer Komponenten oder Verschlüsselungsalgorithmen). Aufgrund dieser Details könnte ein Dritter mit entsprechendem Knowhow möglicherweise die Sicherheitsvorkehrungen überwinden und (Fern-)Zugriff auf das Fahrzeug erhalten und könnte so die Sicherheit des Fahrers sowie der Passagiere massiv gefährden.
- Die Vorschrift könnte auch für den Gesundheitsbereich relevant sein. Herzschrittmacherpatienten etwa, die ihr Implantat über eine App überprüfen und Daten auslesen können, könnten ein Interesse daran haben, dass manche der Daten gerade nicht ausgelesen bzw. jedenfalls nicht an die App übermittelt werden, sondern etwa nur durch ein spezielles Gerät und ärztliches Fachpersonal überprüft werden können. Die Nutzung oder Weitergabe dieser entsprechenden Daten würde die Nutzer gefährden, etwa durch das Wissen um bestimmte arhythmische Herzfunktionalitäten. Dann hätte auch der Nutzer ein Interesse an der Einschränkung. So handelt es sich um Informationen über technische Schnittstellen, deren freie Nutzung aus Gründen der technischen Sicherheit eingeschränkt werden muss.

Nutzer können gegen entsprechende vertragliche Beschränkungen neben der Möglichkeit des Rechtswegs auch gemäß Art. 37 Abs. 5 lit. b Data Act bei der zuständigen Behörde Beschwerden einlegen oder nach Vereinbarung mit dem Dateninhaber eine Streitschlichtungsstelle konsultieren.

Dateninhaber dürfen ihre **Geschäftsgeheimnisse** wahren, sodass eine Offenlegung nur bei Wahrung angemessener Schutzmaßnahmen erfolgt.

Beispiel: Schutz von Geschäftsgeheimnissen

Der Nutzer eines vernetzten Fahrzeugs der Auto AG wendet sich an das Unternehmen als Dateninhaber, um die Daten seines Fahrzeugs zu erhalten. Er verlangt Daten über die Nutzung der im Fahrzeug enthaltenen Fahrerassistenzsysteme (z. B. ESP, Travel Assist, Spurhalteassistent) sowie über Daten zu einzelnen Motoren- und Leistungsmerkmalen heraus. Die Auto AG ist grundsätzlich verpflichtet, die Daten zur Verfügung zu stellen. Lässt sich aber aufgrund der Gesamtheit an Daten auf sensible Geschäftsgeheimnisse schließen, darf die Auto AG diese Daten zurückhalten.

Der Nutzer darf die erhaltenen Daten **nicht für wettbewerbswidrige Zwecke** nutzen. Hierzu gehört die Nutzung zur Entwicklung vernetzter Konkurrenzprodukte.

Beispiel: Wettbewerbswidriges Verhalten

Die Voiture S.E., eine unmittelbare Konkurrentin der Auto AG, erwirbt ein Fahrzeug der Auto AG und möchte damit genaue Informationen zum Fahrzeug erhalten, nur, um ihre eigenen Fahrzeuge zu verbessern. Dies wäre wettbewerbswidrig und nicht vom Data Act umfasst. Ebenso wenig wäre es erlaubt, wenn der Käufer und Nutzer eines solchen Fahrzeugs zugleich Autohändler für Fahrzeuge der konkurrierenden Voiture S.E. ist und die Daten nur nutzt, um sie auf seiner Webseite zu veröffentlichen und damit zu werben, dass Fahrzeuge der Auto AG technisch auf dem „schlechtesten Stand der Welt“ seien und nur ein echtes Voiture das beste Fahrzeug sei.

Ferner ist es dem Nutzer untersagt, Daten durch das Ausnutzen technischer Lücken zu erhalten, Art. 4 Abs. 10 und 11 Data Act.

Beispiel: Treuwidrige Datennutzung

Hat ein Nutzer in Online-Foren erfahren, dass die Sensordaten des Fahrzeugs mittels eines Tricks auf einen angeschlossenen USB-Stick heruntergeladen werden können, indem durch Drücken der Tasten für die beheizbare Heckscheibe und der beheizbaren Windschutzscheibe gleichzeitig eine Fehlfunktion hervorgerufen wird, so wäre es dem Nutzer untersagt, auf diese Weise an die Daten zu gelangen.

5.1.3 Weitergabe von Daten an Dritte, Art. 5 Data Act

Art. 5 Data Act regelt das Recht des Nutzers auf Weitergabe von Daten an Dritte.

So muss der Dateninhaber nach Art. 5 Abs. 1 Data Act auf Verlangen eines Nutzers einem Dritten „ohne Weiteres verfügbare“ Daten sowie die für die Auslegung und Nutzung dieser Daten erforderlichen Metadaten bereitstellen.

Die **konkreten Anforderungen** (unverzüglich, unentgeltlich etc.) werden hier genauso definiert wie bei Art. 4 Abs. 1 Data Act (siehe oben 5.1.2). Damit erweitert der Data Act die rechtliche Position jener Nutzer, die die relevanten Daten nicht selbst nutzen können oder wollen, sondern dies Dritten überlassen möchten.

Beispiel: Datenbereitstellung für Telematiktarif

Der Käufer eines Fahrzeugs der Auto AG wünscht, die regelmäßig von der Auto AG erhobenen Daten der Fahrerassistenzsysteme der Fahrzeug-Versicherung GmbH zur Verfügung zu stellen, um den besonders günstigen Tarif „*Pay How You Drive*“ zu erhalten. Der Käufer verspricht sich als besonders vorsichtigem und umsichtigem Fahrer extrem günstige Beitragsraten für seine Kfz-Versicherung. Für den Käufer und Nutzer muss diese Übermittlung kostenlos erfolgen. Die Fahrzeug-Versicherung GmbH muss die Daten nicht kostenlos erhalten.

Pragmatisch könnte die Fahrzeug-Versicherung GmbH darauf bestehen, dass die Daten zunächst kostenlos an den Nutzer gelangen und dieser die Daten dann an die Fahrzeug-Versicherung GmbH weiterleitet. Dann wäre die Nutzung entgeltfrei möglich. Die Daten für den Nutzer sind aber häufig nicht in einem solchen Format oder werden über eine solche Schnittstelle (API) bereitgestellt, dass sie die Fahrzeug-Versicherung GmbH effizient nutzen kann. Daher dürfte die Fahrzeug-Versicherung GmbH durchaus bereit sein, ein Entgelt für den Datenzugang zu zahlen und dafür die Daten passend verwenden zu können.

Dieser **Weitergabeanspruch gilt** nach Art. 5 Abs. 2 Data Act „**nicht** für (…) Daten im Zusammenhang mit der Prüfung neuer vernetzter Produkte, Stoffe oder Verfahren, die noch nicht in Verkehr gebracht werden, es sei denn, ihre Verwendung durch Dritte ist vertraglich genehmigt.“ Gerade bei der Entwicklung neuer Produkte wird damit den berechtigten Interessen der Hersteller (insbesondere dem Schutz von Geschäftsgeheimnissen) Rechnung getragen.

Ganz allgemein schränkt Art. 5 Abs. 3 Data Act den Weitergabeanspruch ein, indem Unternehmen, die als sog. **Torwächter ("Gatekeeper") im Sinne des Digital Markets Acts** anzusehen sind, aus dem Rechtsbegriff des Dritten herausgenommen werden, also nicht empfangsberechtigt sind. Gatekeeper sind die Betreiber großer Online-Plattformen. Als solche

benannte die EU-Kommission bislang Apple, Alphabet, Meta, Amazon, Microsoft, ByteDance[22] und Booking.[23]

Im Falle von Streitigkeiten regelt Art. 5 Abs. 12 Data Act **Rechtsbehelfe**, wie etwa die Beschwerde bei der zuständigen Stelle gem. Art. 37 Abs. 5 lit. b Data Act oder die Einschaltung. einer Streitbeilegungsstelle.

5.1.4 Datenverarbeitung von Dritten für den Nutzer, Art. 6 Data Act

Auch wenn der Data Act die Weitergabe von Daten an einen Dritten unter den Voraussetzungen des Art. 5 erlaubt, ist deren **Verarbeitungsbefugnis nicht unbeschränkt**. Vielmehr regelt Art. 6 Data Act bestimmte Vorgaben, zum einem im Sinne einer strengen Zweckbindung (Absatz 1), zum anderen im Sinne eines Schädlichkeitsverbots (Absatz 2).

So dürfen Dritte nach Art. 6 Abs. 1 Data Act die ihnen bereitgestellten Daten **nur zu den vereinbarten Zwecken und Bedingungen** verarbeiten. Die Daten sind zu löschen, sobald sie für den vereinbarten Zweck nicht mehr benötigt werden; für nicht personenbezogene Daten ist eine anderslautende Vereinbarung möglich.

Darüber hinaus regelt Art. 6 Abs. 2 Data Act **spezifische Vorgaben und Verbote für Dritte**. Diese umfassen:
- die Nutzer nicht übermäßig in der Ausübung ihrer Wahlmöglichkeiten oder Rechte aus Art. 5 Data Act zu behindern;
- die erhaltenen Daten nicht für Profiling zu nutzen, außer es ist für die Erbringung des vom Nutzer gewünschten Dienstes erforderlich;
- die Daten nicht ohne angemessene Vereinbarungen an andere Dritte weiterzugeben;
- die Daten nicht an als Torwächter definierte Unternehmen i.S.d. Art. 3 DMA weiterzugeben;
- die Daten nicht zur Entwicklung konkurrierender Produkte zu verwenden;
- die Daten nicht so zu verwenden, dass sie die Sicherheit des vernetzten Produkts oder Dienstes gefährden;
- die vereinbarten Maßnahmen zur Wahrung der Vertraulichkeit von Geschäftsgeheimnissen nicht zu missachten
- den Verbraucher nicht daran zu hindern, die erhaltenen Daten an Dritte weiterzugeben.

Beispiel: Nutzungsanalysen

Die (unabhängige) Fahrzeug-Versicherung GmbH aus dem Beispiel zuvor möchte weitere Märkte erschließen und geht eine Partnerschaft mit der Supercar AG ein, einer

[22] Zu diesem chinesischen Konzern, der 2023 einen Umsatz von 120 Mrd. Euro machte, zählt unter anderem TikTok.
[23] https://digital--markets--act-ec-europa-eu.translate.goog/gatekeepers_en?_x_tr_sl=en&_x_tr_tl=de&_x_tr_hl=de&_x_tr_pto=rq#:~:text=On%206%20September%202023%20the,Digital%20Markets%20Act%20(DMA).

unmittelbaren Konkurrentin der Auto AG. Teil der Partnerschaft soll das Teilen sämtlicher Fahrzeugdaten aller versicherten Fahrzeuge sein. Insbesondere will sie detaillierte kundespezifische Nutzungsanalysen erstellen. Solche detaillierten Nutzungsanalysen dürften ein Profiling im Sinne von Art. 4 Nr. 4 DSGVO darstellen und sind der Fahrzeug-Versicherung GmbH untersagt. Die Fahrzeug-Versicherung GmbH darf darüber hinaus die von der Auto AG auf Wunsch des Nutzers erhaltenen Fahrzeugdaten nicht ohne Weiteres an die Supercar AG weiterleiten.

Sodann entschließt sich die Fahrzeug-Versicherung GmbH dazu, aufgrund besonders günstiger Konditionen in einen Datenkooperationsvertrag mit Google Ltd. einzutreten und die Daten mit Google Ltd. zu teilen. Auch dies wäre der Fahrzeug-Versicherung GmbH untersagt, da es sich bei Google um einen Torwächter im Sinne von Art. 3 DMA handelt.

5.1.5 Ausnahmen für Klein- und Kleinstunternehmen, Art. 7 Data Act

Wie auch in anderen Kontexten nicht unüblich, werden Klein- und Kleinstunternehmen durch den Data Act privilegiert, um deren Bürokratiekosten nicht unverhältnismäßig werden zu lassen.

So gelten die im Kapitel II (also Art. 3 bis 6 Data Act, oben Kapitel 5.1.1 bis 5.1.4) genannten Pflichten nicht für Daten, die durch die Nutzung von vernetzten Produkten oder verbundenen Diensten generiert werden, welche durch **Kleinst- und Kleinunternehmen** hergestellt, konzipiert oder erbracht werden.

Dies gilt aber nur, solange diese Unternehmen nicht **Teil einer größeren Unternehmensgruppe** sind und nicht als Unterauftragnehmer für die Herstellung oder Konzeption dieser Produkte oder Dienste beauftragt wurden (Art. 7 Abs. 1 Data Act).

Eine ähnliche Ausnahme gilt für **mittlere Unternehmen**, die weniger als ein Jahr als solche klassifiziert sind, sowie für deren Produkte und Dienste bis zu einem Jahr nach Markteinführung.

Praxishinweis: Definition von Klein- und Kleinstunternehmen

Art. 7 Data Act verweist auf die Definition der Klein- und Kleinstunternehmen nach Artikel 2 des Anhangs der Empfehlung 2003/361/EG (Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen)[24]:

---

[24] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32003H0361.

Danach gelten folgende Mitarbeiterzahlen und finanzielle Schwellenwerte zur Definition der Unternehmensklassen:

– Die Größenklasse der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (KMU) setzt sich aus Unternehmen zusammen, die weniger als 250 Personen beschäftigen und die entweder einen Jahresumsatz von höchstens 50 Mio. EUR erzielen oder deren Jahresbilanzsumme sich auf höchstens 43 Mio. EUR beläuft.
– Innerhalb der Kategorie der KMU wird ein kleines Unternehmen als ein Unternehmen definiert, das weniger als 50 Personen beschäftigt und dessen Jahresumsatz bzw. Jahresbilanz 10 Mio. EUR nicht übersteigt.
– Innerhalb der Kategorie der KMU wird ein Kleinstunternehmen als ein Unternehmen definiert, das weniger als 10 Personen beschäftigt und dessen Jahresumsatz bzw. Jahresbilanz 2 Mio. EUR nicht überschreitet.

5.1.6 Vereinbarung über Bereitstellung der Daten zwischen Dateninhaber und Datenempfänger

Der Dateninhaber kann mit dem Datenempfänger die **Bedingungen für die Bereitstellung der Daten** vereinbaren, Art. 8 Data Act.

Auch ist hier der Datenempfänger **regelmäßig nicht exklusiv empfangsberechtigt**, es sei denn, der Nutzer wünscht dies so, Art. 8 Abs. 4 Data Act. Dateninhaber und Datenempfänger brauchen keine Informationen herauszugeben, die über das hinausgehen, was erforderlich ist, um die Einhaltung der für die Datenbereitstellung vereinbarten Vertragsbedingungen oder die Erfüllung ihrer Pflichten aus der Data Act zu überprüfen, Art. 8 Abs. 5 Data Act. Dabei darf auch hier der Dateninhaber grundsätzlich Geschäftsgeheimnisse wahren, Art. 8 Abs. 6 Data Act.

Beispiel: Inhalt eines Datenbereitstellungsvertrags

Die Auto AG als Dateninhaber würde mit der Fahrzeug-Versicherung GmbH einen detaillierten Vertrag über die Art und Weise der Bereitstellung schließen. Die Fahrzeug-Versicherung GmbH dürfte nicht verlangen, dass die Auto AG ausschließlich mit ihr als Vertreter der Kfz-Versicherungsbranche die Daten übermittelt. Sinnvoll wären hingegen Regelungen zu den technischen Übermittlungswegen, dem Übermittlungszeitraum und -frequenz etc.

Entscheidend ist, dass der Dateninhaber vom **Datenempfänger** für die Bereitstellung der Daten ein **Entgelt** verlangen darf. Diese muss gemäß Art. 9 Abs. 1 Data Act allerdings angemessen sein. Dies ist ein wesentlicher Unterschied zur Herausgabe **an den Nutzer**, da die Herausgabe an den Nutzer im Grunde **kostenlos** zu erfolgen hat, vgl. Art. 4 Abs. 1 Data Act.

Beispiel: Kostenlose Datenbereitstellung versus angemessene Vergütung

Der Fahrer des Auto-AG-Fahrzeugs hat Anspruch auf kostenlosen Zugang zu den erzeugten Daten, die Fahrzeug-Versicherungs GmbH gerade nicht. In dem Vertrag zwischen der Auto AG und der Fahrzeug-Versicherungs GmbH dürfte die Auto AG eine angemessene Vergütung verlangen.

Das verlangte Entgelt muss **angemessen** sein und soll keine Kompensation für den Wert der Daten per se darstellen. Bei der Berechnung der Höhe sind vielmehr Aspekte zu berücksichtigen wie: angefallene Kosten für die Bereitstellung der Daten, einschließlich insbesondere der notwendigen Kosten für die Formatierung der Daten, die Verbreitung auf elektronischem Wege und die Speicherung, gegebenenfalls Investitionen in die Erhebung und Generierung von Daten, wobei berücksichtigt wird, ob andere Parteien zur Beschaffung, Generierung oder Erhebung der betreffenden Daten beigetragen haben.

5.2 Datenbereitstellung für öffentliche Stellen

Nachdem der Data Act weitgehend die Rechtsbeziehungen zwischen privaten Nutzern und Unternehmen sowie zwischen Unternehmen regelt, enthält er in den Art. 14 ff. einen eigenen Abschnitt zur Datenbereitstellung für öffentliche Stellen. Während das Ziel der Nutzung bereitgestellter Daten im Privatsektor heterogen sein kann, geht es bei der Pflicht zur Bereitstellung an öffentliche Stellen nur um die Bewältigung von Notlagen. Der Data Act spricht hier von der „außergewöhnlichen Notwendigkeit der (behördlichen) Datennutzung“.

5.2.1 Berechtigte Stellen

Der besondere Anspruch auf Datenbereitstellung in Notlagen gilt nur für Öffentliche Stellen im Sinne des Art. 2 Nr. 28 Data Act, also jede nationale, regionale und lokale **Behörde**, **Körperschaft** und **Einrichtung des öffentlichen Rechts** der Mitgliedstaaten, aber auch **Verbände**, die aus einer oder mehreren dieser Behörden, Körperschaften oder Einrichtungen bestehen (wie etwa ein kommunaler Zweckverband). Zu den berechtigten Adressaten gehören neben öffentlichen Stellen auch die Kommission, die europäische Zentralbank und Einrichtungen der Union.

Wenn eine der genannten Stellen den **Nachweis** erbringt, dass für die „Erfüllung ihrer rechtlichen Aufgaben im öffentlichen Interesse die außergewöhnliche Notwendigkeit der Nutzung bestimmter Daten – einschließlich der für die Auslegung und Nutzung dieser Daten erforderlichen betreffenden Metadaten – gemäß Artikel 15 besteht, stellen die Dateninhaber, bei denen sich diese Daten befinden …, diese Daten auf ordnungsgemäß begründeten Antrag bereit.“ (Art. 14 Data Act)

Bei den Dateninhabern muss „es sich um andere juristische Personen als öffentliche Stellen“ handeln. Das bedeutet, dass sich öffentliche Stellen für ein Datenbereitstellungsverlangen nicht untereinander auf die Art. 14 ff. Data Act berufen können. Stattdessen kommt etwa ein Verfahren der Amtshilfe in Betracht.

Wann die **außergewöhnliche Notwendigkeit der Datennutzung** bestehen kann, wird in Art. 15 Abs. 1 Data Act näher bestimmt. Dies betrifft insbesondere den **öffentlichen Notstand.** Nach Art. 2 Nr. 29 Data Act ist *„öffentlicher Notstand“ eine zeitlich begrenzte Ausnahmesituation – wie etwa Notfälle im Bereich der öffentlichen Gesundheit, Notfälle infolge von Naturkatastrophen sowie von Menschen verursachte Katastrophen größeren Ausmaßes, einschließlich schwerer Cybersicherheitsvorfälle –, die sich negativ auf die Bevölkerung der Union oder eines Mitgliedstaats bzw. eines Teils davon auswirkt, das Risiko schwerwiegender und dauerhafter Folgen für die Lebensbedingungen, die wirtschaftliche Stabilität oder die finanzielle Stabilität oder die Gefahr einer erheblichen und unmittelbaren Beeinträchtigung wirtschaftlicher Vermögenswerte in der Union oder in dem betroffenen Mitgliedstaat birgt und die nach den einschlägigen Verfahren des Unionsrechts oder des nationalen Rechts festgestellt und amtlich ausgerufen wurde*.“

Vorliegen muss also dreierlei:

– eine zeitlich begrenzte Ausnahmesituation
– das Risiko schwerwiegender und dauerhafter Folgen für die Lebensbedingungen
– die amtliche Feststellung und Ausrufung des Notstands

Beispiel: Datenherausgabe bei Cyberangriff

Die Fahrer der vernetzten Fahrzeuge der Auto AG sind allesamt Opfer eines Cyberangriffes geworden, da sich die internationale Hackergruppe „Pseudonymous“ durch Ausnutzung einer Schwachstelle in der Fahrzeugsoftware Fern-Zugriff zu allen Fahrzeugen verschafft hat und diese individuell steuern kann. Gleichzeitig prahlt die Gruppe auf diversen Nachrichtenportalen damit und avisiert, dass die Fahrer betroffener Fahrzeuge bald noch ihr „blaues Wunder erleben“ werden. Die zuständige Behörde verlangt Fahrzeugdaten und Informationen der Schnittstellen unverzüglich von der Auto AG heraus, da sie nur so in der Kürze der Zeit an die Daten gelangen, aufgrund der eingesetzten Technologien und Formate die Sicherheitslücke auffinden und schließlich Gegenmaßnahmen ergreifen kann, um Schaden für Leib und Leben der Teilnehmer am Straßenverkehr abzuwenden. Die Auto AG muss der zuständigen Behörde Zugang zu den Daten verschaffen.

Es gibt **weitere Fälle einer speziellen Datenbereitstellungspflicht** für öffentliche Stellen.

So sind Dateninhaber nach Art. 15 Abs. 1 lit. b Data Act zur Bereitstellung verpflichtet, wenn die öffentliche Stelle

– spezifische nicht-personenbezogene Daten ermittelt hat,

– ihr Fehlen sie daran hindert, eine bestimmte im öffentlichen Interesse liegende Aufgabe zu erfüllen
– die Datennutzung aber rechtlich ausdrücklich vorgesehen ist.

Darüber hinaus kann eine Datenbereitstellungspflicht gegenüber öffentlichen Stellen ausgelöst werden, wenn

– die öffentliche Stelle alle ihr zur Verfügung stehenden Mittel ausgeschöpft haben, um entsprechende Daten zu erlangen, darunter der **Erwerb von nicht personenbezogenen Daten auf dem Markt** durch Angebot von Markttarifen[25] oder
– die **Inanspruchnahme bestehender Verpflichtungen** zur Bereitstellung von Daten oder
– der **Erlass neuer Rechtsvorschriften**, die die rechtzeitige Verfügbarkeit der Daten gewährleisten könnte.

Beispiel: Datenherausgabe bei Verkehrsunfällen

Verschiedene Fahrzeuge der Auto AG sind vermehrt an Straßenverkehrsunfällen beteiligt. Grund für die Unfälle scheint nach Prüfung der jeweiligen Fälle eine Fehlfunktion der elektronischen und computerunterstützten Bremsanlage zu sein. Um nicht wahllos weitere Fahrzeuge per Zufallsprinzip zu untersuchen, verlangt die zuständige Behörde von der Auto AG sämtliche die Fahrzeuge betreffenden Daten heraus. Ein solches Begehren wäre allerdings nicht mehr verhältnismäßig, da nicht jegliches Datum des Fahrzeugs zu einem Erkenntnisgewinn hinsichtlich der Unfallursache führen würde. Gleichwohl darf die Behörde Daten in Bezug zur Fahrzeugbremsanlage herausverlangen, um hieraus Rückschlüsse auf die Fehlfunktion zu erhalten.

Dabei müsste die zuständige Behörde aber zunächst versuchen, mit Skizzen oder Beschreibungen der Bremsanlage selbst den Fehler zu rekonstruieren. Gelingt dies jedoch nicht, da es sich etwa um einen Fahrzeug-Interoperabilitätsfehler handelt, der aus den Dokumentationen nicht ersichtlich ist, darf die Behörde die oben genannten Daten herausverlangen.

Klein- und Kleinstunternehmen unterliegen nicht dieser Bereitstellungspflicht, Art. 15 Abs. 2 Data Act.

In allen geschilderten Fällen einer außergewöhnlichen Notwendigkeit der Nutzung bestimmter Daten ist zu beachten, dass diese immer **zeitlich befristet** sein muss. Die Dauer dieser spezifischen Datenbereitstellungspflicht richtet sich nach den jeweils genannten Umständen.

[25] Die Verpflichtung nachzuweisen, dass die nicht personenbezogenen Daten nicht auf dem Markt erworben werden konnten, muss die öffentliche Stelle nicht erfüllen, wenn die spezifische Aufgabe, die im öffentlichen Interesse ausgeübt wird, in der Erstellung amtlicher Statistiken besteht und der Erwerb solcher Daten nach nationalem Recht nicht zulässig ist, Art. 15 Abs. 3 Data Act.

5.2.2 Art der Daten

Die berechtigten Stellen können in einem Notfall gemäß Art. 15 Abs. 1 lit. b Data Act lediglich solche Daten herausverlangen, die **nicht personenbezogen** sind. Die Übermittlung personenbezogener Daten in diesem Kontext ist gemäß Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO i.V.m. Art. 14 Data Act nicht gerechtfertigt. Die Abgrenzung kann zuweilen schwierig sein, weil auch vermeintlich nicht-personenbezogene Daten je nach Kontext auch einen Personenbezug erhalten können (wie etwa Daten der Sensoren aus einem Fahrzeug, die auch Rückschlüsse auf das Fahrverhalten zulassen). Man muss allerdings auch beachten, dass es sich bei den Daten, die eine öffentliche Stelle in einem Katastrophenfall benötigt, nicht unbedingt um solche aus vernetzten Produkten handelt, sondern etwa um Daten zu Produkten, die zur Gefahrenabwehr benötigt werden (wie etwa das Auskunftsverlangen in der Pandemie, wieviele Masken ein Unternehmen kurzfristig herstellen kann).

5.2.3 Anforderung an Datenbereitstellungsverlangen

Die (berechtigte) öffentliche Stelle muss einen Antrag an den Dateninhaber stellen, der alle **formellen Voraussetzungen des Datenverlangens** erfüllt. Nach Art. 17 Abs. 2 Data Act muss der Antrag

- **schriftlich** und in klarer, prägnanter, einfacher und für den Dateninhaber verständlichen Sprache abgefasst sein
- im Hinblick auf die Detailstufe, Umfang und Häufigkeit des Zugangs angemessen und gut begründet werden, insbesondere den **Nachweis der außergewöhnlichen Notwendigkeit** nach Art. 14 Data Act erbringen
- genaue **Angaben zur Art der verlangten Daten** machen, die der Dateninhaber bereitstellen soll, Art. 17 Abs. 2 lit. b Data Act
- den **Zweck der Datenanfrage**, die beabsichtigte Nutzung der Daten, auch durch Dritte, und die Nutzungsdauer erläutern, Art. 17 Abs. 1 lit. c Data Act.
- darlegen, wann die Daten voraussichtlich gelöscht werden (Art. 17 Abs. 1 lit. d Data Act).
- über mögliche **Sanktionen** informieren, falls der Dateninhaber dem Verlangen nicht nachkommt, Art. 17 Abs. 2 lit. f Data Act.
- angegeben werden, welche **anderen Stellen oder Dritte Zugang** zu den bereitgestellten Daten erhalten, Art. 17 Abs. 1 lit. f Data Act.
- die Rechtsvorschrift, die die **Aufgabe** im öffentlichen Interesse der öffentlichen Stelle zuweist (Art. 17 Abs. 1 lit. h Data Act) und die **Frist** für die Bereitstellung der Daten angeben (Art. 17 Abs. 1 lit. i Data Act).

- und bei allem die rechtmäßigen Ziele des Dateninhabers respektieren sowie die Wahrung von Geschäftsgeheimnissen garantieren, Art. 17 Abs. 2 lit. d Data Act.

Die Kommission wird ein **Musterformular** entwickeln, das die zuvor genannten Voraussetzungen aufgreifen wird, Art. 17 Abs. 6 Data Act.

Beispiel: Begründung für Herausgabeverlangen

Verlangt im Beispiel zuvor die zuständige Behörde die Daten dem Grunde nach rechtmäßig heraus, so muss sie zur Geltendmachung ihr Begehren plausibel begründen. Die oben beschriebenen Umstände müssen sich in der Begründung wiederfinden. Zudem muss die zuständige Behörde der Auto AG garantieren, dass sie die erhaltenen Daten der Bremsanlage umfassend technisch schützen und etwaige aus den Daten und der Untersuchung offenbar werdende Geschäftsgeheimnisse gegenüber Dritten wahren wird.

Grundsätzlich bezieht sich das Datenverlangen auf **nicht-personenbezogene Daten**. Nach Art. 17 Abs. 2 lit. e Data Act können aber auch **personenbezogene Daten** unter Berücksichtigung entsprechender technischer und organisatorischer Schutzmaßnahmen in pseudonymisierter Form angefordert werden. Bei solchen Anfragen sind die **erforderlichen technischen und organisatorischen Maßnahmen**, die für die Einhaltung des Datenschutzes erforderlich sind, zu spezifizieren, Art. 17 Abs. 1 lit. g Data Act. Ein Verlangen auf Bereitstellung personenbezogener Daten muss nach Art. 17 Abs. 2 lit. i Data Act **der zuständigen Aufsichtsbehörde gemeldet** werden.

Sämtliche Anträge auf Datenbereitstellung müssen dem zuständigen Datenkoordinator **übermittelt und online veröffentlicht** werden, es sei denn, dies birgt ein Sicherheitsrisiko, Art. 17 Abs. 2 lit. g Data Act.

Öffentliche Stellen müssen sich bemühen, **Haftungsrisiken** für den Dateninhaber **zu vermeiden**, Art. 17 Abs. 1 lit. j Data Act.

5.2.4 Datenbereitstellung durch Dateninhaber

Wenn ein Dateninhaber einen (rechtmäßigen) Antrag einer öffentlichen Stelle auf Datenbereitstellung erhalten hat, muss er die angefragten Daten unverzüglich bereitstellen. Die näheren Anforderungen an die **Erfüllung des Datenverlangens durch den Dateninhaber** sind in Art. 18 Data Act geregelt.

Ein Dateninhaber kann das Datenverlangen unter bestimmten Bedingungen ablehnen oder dessen Änderung beantragen, Art. 18 Abs. 2 Data Act.

Als **Gründe für eine Ablehnung oder Änderung** nennt Art. 18 Abs. 2 Data Act:

- Der Dateninhaber hat keine Kontrolle über die angeforderten Daten,
- ein ähnliches Verlangen wurde bereits gestellt und es wurde nicht über das Löschen der Daten informiert, oder
- das Verlangen erfüllt nicht die Voraussetzungen nach Art. 17 Abs. 1 und 2 Data Act.

Die Ablehnung des Begehrens bzw. der Antrag auf Änderung müssen bei öffentlichen Notständen **unverzüglich** und **innerhalb von fünf Arbeitstagen**, bei anderen außergewöhnlichen Notwendigkeiten innerhalb von **30 Arbeitstagen** nach Eingang des Antrags erfolgen.

Praxishinweis: Entschädigung für Datenbereitstellung

Grundsätzlich hat die Datenbereitstellung bei einem öffentlichen Notstand **unentgeltlich** zu erfolgen, Art. 20 Abs. 1 Data Act (Ausnahme: Kleinst- und Kleinunternehmen). Der Dateninhaber wird jedoch – sollte er dies wünschen – **öffentlich** hierfür durch die öffentlichen Stellen **gewürdigt**. In den übrigen Fällen einer Datenbereitstellung hat der Dateninhaber einen **Anspruch auf eine faire Gegenleistung** für die Bereitstellung der Daten.

Art. 20 Abs. 4 Data Act regelt eine Ausnahme für die Entschädigung. Es besteht dann **kein Anspruch auf eine Gegenleistung** für die Bereitstellung von Daten, wenn die besondere Aufgabe im öffentlichen Interesse in der Erstellung amtlicher Statistiken darstellt und der Erwerb von Daten nach nationalem Recht unzulässig ist.

5.2.5 Datennutzung durch öffentliche Stellen

Wie die öffentlichen Stellen mit den bereitgestellten Daten verfahren dürfen, regelt Art. 19 Data Act. Danach

- darf die öffentliche Stelle die Daten nicht in einer Weise nutzen, die mit dem Zweck des Datenverlangens unvereinbar ist, insbesondere auch nicht öffentlich machen[26];
- muss sie technische und organisatorische Maßnahmen treffen, die die Vertraulichkeit und Integrität der verlangten Daten und die Sicherheit der Datenübermittlungen – insbesondere bei personenbezogenen Daten – wahren und die Rechte und Freiheiten der betroffenen Personen schützen (vgl. Art. 19 Abs. 4 Data Act);
- muss sie die Daten im Regelfall löschen, sobald sie für den angegebenen Zweck nicht mehr erforderlich sind, und dies dem Dateninhaber unverzüglich mitteilen.

Praxishinweis: Geschäftsgeheimnisse

Nach Art. 19 Abs. 3 Data Act gilt die Offenlegung von Geschäftsgeheimnissen gegenüber einer öffentlichen Stelle nur in dem Maße als erforderlich, in dem dies für den Zweck eines Verlangens gemäß Artikel 15 unerlässlich ist. In diesem Fall muss der Dateninhaber oder, falls es sich dabei nicht um dieselbe Person handelt, der Inhaber des Geschäftsgeheimnisses die Daten, die als Geschäftsgeheimnisse geschützt sind, einschließlich der

[26] Insoweit finden die entsprechenden Vorschriften aus Art. 3 ff. DGA und der RL (EU) 2019/1024 und nationale Umsetzungsgesetze, wie das Datennutzungsgesetz, keine Anwendung.

einschlägigen Metadaten, identifizieren. Die öffentliche Stelle trifft vor der Offenlegung von Geschäftsgeheimnissen alle erforderlichen und geeigneten technischen und organisatorischen Maßnahmen, um die Vertraulichkeit der Geschäftsgeheimnisse zu wahren, gegebenenfalls einschließlich der Verwendung von Mustervertragsbestimmungen, technischen Normen und der Anwendung von Verhaltenskodizes.

Die empfangende öffentliche Stelle ist befugt, die bereitgestellten Daten einer anderen öffentlichen Stelle zwecks Wahrnehmung der in Art. 15 Data Act präzisierten **Aufgaben im öffentlichen Interesse** zu übermitteln.

Außerdem dürfen entsprechende Daten nach der Maßgabe des Art. 21 Data Act an **Forschungseinrichtungen** oder statistische Ämter weitergegeben werden.

5.3 Wechselerleichterung zwischen Datenverarbeitungsdiensten

Wie schon eingangs gesehen, gehören Datenverarbeitungsdienste zu den zentralen Dienstleistungen im Ökosystem des Data Acts. Hierzu gehören digitale Dienstleistungen, die einem Kunden bereitgestellt werden und einen flächendeckenden und auf Abruf verfügbaren Netzzugang zu einem gemeinsam genutzten Pool konfigurierbarer, skalierbarer und elastischer Rechenressourcen ermöglicht – zum Beispiel Clouddienste, in denen jene Daten vorgehalten werden, die im Rahmen des Data Acts bereitzustellen sind.

Kapitel VI regelt hierzu den Wechsel von Datenverarbeitungsdiensten, genauer: dessen Erleichterung aus Sicht der Nutzer. Dementsprechend haben Anbieter von Datenverarbeitungsdiensten Maßnahmen zu treffen, um den Kunden eine größtmögliche Autonomie im Hinblick auf die besagten Dienste zu ermöglichen. Hierzu zählen insbesondere die Freiheit,

- zu einem Datenverarbeitungsdienst, der die gleiche Dienstart abdeckt, die von einem anderen Anbieter von Datenverarbeitungsdiensten erbracht wird, zu wechseln
- zu einer IKT-Infrastruktur in eigenen Räumlichkeiten zu wechseln
- oder auch mehrere Anbieter von Datenverarbeitungsdiensten gleichzeitig in Anspruch zu nehmen.

Dabei dürfen Anbieter von Datenverarbeitungsdiensten keine **vorkommerziellen, gewerblichen, technischen, vertraglichen und organisatorischen Hindernisse** aufzwingen und müssen solche Hindernisse beseitigen. Hierzu zählen etwa unredliche Kündigungsfristen, die Verhinderung oder Erschwerung des Datenexports, der Erzielung einer Funktionsäquivalenz oder der Trennung von einzelnen Diensten, soweit dies technisch durchführbar ist.

Um all dies auch vertraglich abzusichern, verpflichtet Art. 25 Data Act zur Verwendung bestimmter, dort in Absatz 2 näher spezifizierter **Vertragsklauseln**.

Praxishinweis: Vertragsklauseln zum Wechsel von Datenverarbeitungsdiensten

Zu den Vertragsklauseln, die Art. 25 Abs. 2 Data Act aufführt, zählen etwa:

- Klauseln, die es dem Kunden ermöglichen, **auf Verlangen** zu einem Datenverarbeitungsdienst **zu wechseln**, der von einem anderen Anbieter von Datenverarbeitungsdiensten angeboten wird
- die Verpflichtung des Anbieters von Datenverarbeitungsdiensten, die für die vertraglich vereinbarten Dienste relevante **Ausstiegsstrategie des Kunden zu unterstützen**, unter anderem durch Bereitstellung aller einschlägigen Informationen
- eine Klausel, in der festgelegt ist, dass der **Vertrag als beendet gilt**, nachdem der Wechsel erfolgreich vollzogen ist oder nach Ablauf der maximalen Kündigungsfrist von 2 Monaten:
- eine erschöpfende **Auflistung aller Kategorien von Daten und digitalen Vermögenswerten**, die während des Wechselvollzugs übertragen werden können
- eine **Mindestfrist für den Datenabruf** von mindestens 30 Kalendertagen
- eine Klausel, die garantiert, dass alle **exportierbaren Daten und digitalen Vermögenswerte**, die direkt vom Kunden generiert werden oder sich direkt auf den Kunden beziehen, nach Ablauf des Abrufzeitraums oder nach Ablauf eines vereinbarten alternativen Zeitraums **vollständig gelöscht** werden, sofern der Wechsel erfolgreich vollzogen ist

Darüber hinaus werden den Anbietern von Datenverarbeitungsdiensten eine ganze Reihe von **Informationspflichten** auferlegt, Art. 26 und Art. 28 Data Act. Diese betreffen etwa

- Informationen über mögliche **Verfahren für den Wechsel** und die Übertragung der Inhalte
- die Nennung verfügbarer **Methoden und Formate** sowie Einschränkungen und technische Beschränkungen.
- die Aufnahme eines Hinweises auf ein aktuelles **Online-Register des Datenverarbeitungsdienstes,** in dem die Einzelheiten zu allen Datenstrukturen und Datenformaten sowie den einschlägigen Normen und offenen Interoperabilitätsspezifikationen verfügbar sind, Art. 26 Data Act
- Informationen über die **Gerichtsbarkeit**, denen die IKT-Infrastruktur unterliegt
- eine allgemeine Beschreibung der **technischen, organisatorischen und vertraglichen Maßnahmen**, die ein Anbieter getroffen hat, um einen nach EU-Recht bzw. dem Recht eines europäischen Mitgliedstaats unrechtmäßigen internationalen staatlichen Zugang auf nicht personenbezogene Daten bzw. eine entsprechende Übermittlung dieser Daten zu verhindern.

Praxishinweis

Die in Art. 26 und 28 Data Act genannten Informationspflichten treffen nur die Anbieter von Datenverarbeitungsdiensten und sind von jenen Informationspflichten zu

unterscheiden, die den Hersteller nach den Art. 3 ff. Data Act treffen (hierzu bereits oben 5.1). Die Informationen werden auf den Websites der Anbieter bereitgestellt und dort auf dem neuesten Stand gehalten.

Um einen redlichen Umgang der Akteure zu erreichen und die Rechtzeitigkeit der Datenübertragung sowie die Kontinuität der Leistung sicherzustellen, zwingt Art. 27 Data Act die Datenverarbeitungsdienste zur Zusammenarbeit, genauer gesagt: appelliert diese Vorschrift an den **Grundsatz von Treu und Glauben**.

Einer der bisherigen Streitpunkte im Wettbewerb zwischen Datenverarbeitungsdiensten ist die Erhebung eines Wechselentgelts, um Kunden nicht all zu leicht ziehen zu lassen. Diese dürfen ab der Geltung des Data Acts (12.09.2025) bis zum 12.01.2027 noch mit der Maßgabe erhoben werden, dass sie nur die Kosten abdecken, die unmittelbar im Zusammenhang mit dem betreffenden Wechsel entstehen, Art. 29 Abs. 2 und 3 Data Act. Nach diesem Zeitpunkt sind Wechselentgelte abgeschafft.

Eine Ausnahme regelt insoweit Art. 31 Data Act. Danach finden die Regulierung zum Wechselentgelt und zu technischen Vorgaben des Wechselns keine Anwendung **für bestimmte Datenverarbeitungsdienste**, etwa solche, bei denen die meisten zentralen Funktionen auf die spezifischen Bedürfnisse eines einzelnen Kunden zugeschnitten wurden. Damit wird gleichsam die Investition geschützt, die ein Dienst für die besondere Kundenspezifikation tätigt. Diese Konzeption ähnelt etwas der Regelung des Ausschlusses eines Verbraucherwiderrufs beim Kauf von Produkten, die nach einer **Kundenspezifikation** angefertigt werden (und somit nicht anderweitig veräußert werden können, wie etwa maßgeschneiderte Kleidung oder Produkte mit einer persönlichen Gravur).

Die Einschränkungen in diesem Abschnitt gelten nicht für jene Datenverarbeitungsdienste, die nur zu **Test- und Bewertungszwecken für einen begrenzten Zeitraum** bereitgestellt werden, Art. 31 Abs. 2 Data Act. Anbieter solcher Dienste müssen nach Art. 31 Abs. 3 Data Act vor Vertragsschluss über jene Verpflichtungen informieren, die im jeweiligen Fall nicht zur Anwendung kommen.

5.4 Interoperabilitätsnormen für Daten

Der letzte Abschnitt vor dem Schlusskapitel zu Durchsetzung und Rechtsschutz befasst sich mit dem für den Datenaustausch wichtigen Thema der Interoperabilität.

Interoperabilität ist nach Art. 2 Nr. 40 *die Fähigkeit von zwei oder mehr Datenräumen oder Kommunikationsnetzen, Systemen, vernetzten Produkten, Anwendungen, Datenverarbeitungsdiensten oder Komponenten, Daten auszutauschen und zu nutzen und ihre Funktionen auszuführen*.

Die Art. 33 ff. Data Act bestimmen die wesentlichen Anforderungen an die Interoperabilität von Daten, Mechanismen und Diensten für die Datenweitergabe. Diese Anforderungen

an die Interoperabilität gelten auch für die Bereitstellung von Datensätzen in gemeinsamen europäischen Datenräumen. Das ist insofern von besonderer praktischer Bedeutung, als die Teilnehmer an Datenräumen, die Daten oder Datendienste anbieten, die in Art. 33 Abs. 1 Data Act enumerativ aufgezählten **Anforderungen** erfüllen müssen, um den **Datenaustausch zu vereinfachen**.

Das betrifft insbesondere

- die Bereitstellung detaillierter Informationen über den Inhalt,
- die Bereitstellung der Nutzungsbedingungen
- Informationen über die Qualität der Daten
- Das öffentliche Zugänglichmachen und die einheitliche Darstellung der Struktur und des Formats der Daten
- Die Beschreibung der technischen Mittel für den Datenzugang, wie Programmierschnittstellen und deren Nutzungsbedingungen
- Die Bereitstellung der Mittel für die Interoperabilität von Tools für automatisierte bzw. intelligente Verträge, soweit solche betroffen sind.

In Art. 36 Data Act werden schließlich die Voraussetzungen an intelligente Verträge zur **Ausführung von Datenweitergabevereinbarungen** aufgestellt.

Als **intelligenter Vertrag** wird nach Art. 2 Nr. 39 Data Act ein Computerprogramm bezeichnet, das für die automatisierte Ausführung einer Vereinbarung oder eines Teils davon verwendet wird, wobei eine Abfolge elektronischer Datensätze verwendet wird und die Integrität dieser Datensätze sowie die Richtigkeit ihrer chronologischen Reihenfolge gewährleistet werden.

Danach müssen Anbieter von Datenverarbeitungsdiensten, die intelligente Verträge nutzen, sicherstellen, dass diese **robust** sind und **effektive Zugangskontrollen** bieten, um Fehler und Manipulationen zu verhindern.

Zu den Maßnahmen zählen etwa

- Mechanismen, die Ausführungen von Transaktionen sicher beenden bzw. diese unterbrechen
- die Archivierung von Transaktionsdaten, Logik und Programmcode des intelligenten Vertrags, um eine Nachvollziehbarkeit zu gewährleisten
- der Schutz intelligenter Verträge durch strenge Zugangskontrollen
- Kohärenz mit den Bedingungen der Datenweitergabevereinbarung, die mit dem intelligenten Vertrag umgesetzt wird, Art. 36 Abs. 1 Data Act.

Praxishinweis

Dem Expertenkreis Transformation der Automobilwirtschaft zufolge sollte die Bereitstellung der Daten über eine einheitliche Infrastruktur erfolgen (z. B. *Mobilithek* oder *Mobility Data Space*); als einheitliches Datenformat bietet sich *COVESA VSS* an.[27]

[27] Handlungsempfehlungen zur Erhöhung der Datennutzung und für die Umsetzung einer möglichen sektoralen Regulierung vom 20.09.2023, S. 6 https://expertenkreis-automobilwirtschaft.de/media/pages/home/417c83417c-1695210129/expertenkreis-transformation-der-automobilwirtschaft_kurzpapier_datennutzung.pdf.

6 Checkliste

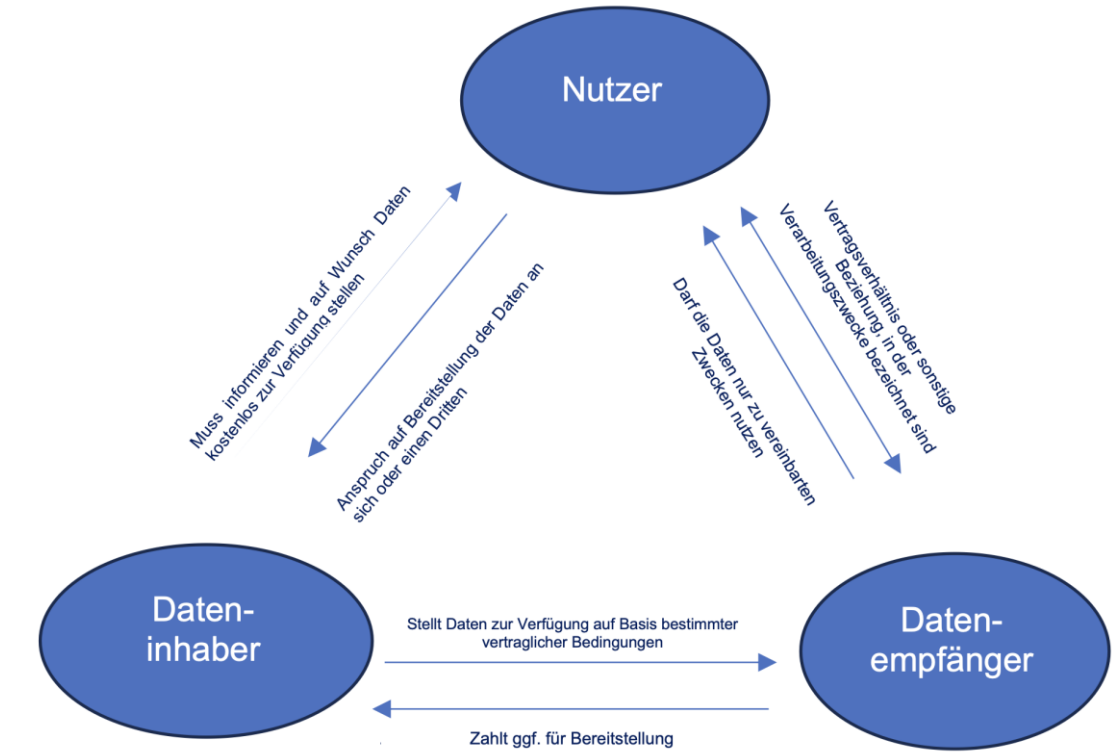
Empfehlungen für die rechtskonforme Umsetzung des Data Act

Die wesentlichen Pflichten, die sich für Unternehmen aus dem Data Act ergeben, werden hier noch einmal zusammengefasst:

- Der Data Act gilt ab dem 12.9.2025. Man sollte sich aber schon vorher mit den wesentlichen Regelungen vertraut machen, nicht zuletzt, um das eigene Geschäftsmodell abzugleichen – sowohl was die Chancen, aber auch die Risiken durch das neue Recht betrifft.
- Praktisch jedes Unternehmen kann von den Neuregelungen betroffen sein.
- Das gilt in erster Linie für die Hersteller vernetzter Produkte und die Anbieter verbundener Dienste. Diese müssen ihre Produkte bzw. Dienste so konzipieren und herstellen bzw. 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 (Art. 3 Abs. 1 Data Act).
- Diesbezüglich müssen sie die Nutzer umfassend informieren (Art. 3 Abs. 2 Data Act).
- Aber auch, wenn man solche (verbundene) Produkte nicht selbst herstellt oder entsprechende Dienste nicht anbietet, kann man als sog. Dateninhaber verpflichtet sein. Als solche gelten Unternehmen, die Daten während der Erbringung eines verbundenen Dienstes abrufen oder generieren, also von dieser Vernetzung im „Internet der Dinge“ profitieren.
- Dateninhaber müssen dem Nutzer ohne Weiteres verfügbare Daten unverzüglich, einfach, sicher, unentgeltlich, in einem umfassenden, gängigen und maschinenlesbaren Format und in der gleichen Qualität wie für den Dateninhaber kontinuierlich und in Echtzeit bereitstellen (Art. 4 Abs. 1 Data Act).
- Auf Verlangen des Nutzers müssen solche Daten auch Dritten weitergegeben werden (Art. 5 Data Act). Nutzer können Verbraucher sein, aber auch Unternehmen.
- Soweit Unternehmen Daten aus vernetzten Produkten oder verbundenen Diensten zu beruflichen bzw. gewerblichen Zwecken (weiter-) verwenden, unterliegen die vertraglichen Beziehungen zwischen ihnen als Datenempfänger und den Dateninhabern gesetzlichen Beschränkungen. So muss insbesondere die Bereitstellung der Daten zu fairen, angemessenen und nichtdiskriminierenden Bedingungen und in transparenter Weise ausgestaltet werden (Art. 8 Data Act).
- Soweit eine außergewöhnliche Notlage (wie etwa eine Pandemie, ein Großschadenereignis etc.) besteht, müssen Unternehmen den zuständigen öffentlichen Stellen insbesondere die für die Gefahrenabwehr notwendigen Sachdaten bereitstellen. Die Wahrung von Geschäftsgeheimnissen ist zu gewährleisten (Art. 14 DataAct).

Um dies noch einmal zu kondensieren, fasst die nachfolgende Grafik das in der Praxis besonders relevante „Dreiecksverhältnis“ von (privaten) Nutzern, Dateninhabern und Datenempfängern zusammen.

Abbildung 4
Rechtsverhältnisse von Nutzer, Dateninhaber und Datenempfänger



Quelle: © Dirk Heckmann

Ansprechpartner/Impressum

Christine Völzow
Geschäftsführerin, Leiterin Abteilung Wirtschaftspolitik

Telefon 089-551 78-251
christine.voelzow@vbw-bayern.de

Johanna Yaacov
Abteilung Wirtschaftspolitik

Telefon 089-551 78-135
johanna.yaacov@vbw-bayern.de

Impressum
Alle Angaben dieser Publikation beziehen sich ohne jede Diskriminierungsabsicht grundsätzlich auf alle Geschlechter.

Herausgeber

vbw
Vereinigung der Bayerischen
Wirtschaft e. V.

Max-Joseph-Straße 5
80333 München

www.vbw-bayern.de

Weiterer Beteiligter

Prof. Dr. Dirk Heckmann

heckmann@mein-jura.de