29.04.2025

Der Data Act als Herausforderung für den Datenschutz

Daten nicht nur schützen, sondern unter Umständen auch teilen – diese Aufgabe kommt ab September 2025 auf Unternehmen zu. Die als europäischer Data Act bezeichnete Verordnung über harmonisierte Vorschriften für den fairen Zugang zu und die faire Nutzung von Daten ist dann als unmittelbar geltendes Recht umzusetzen. Dies erfordert eine Auseinandersetzung mit den neuen Pflichten im Vorfeld auch und insbesondere durch die Beschäftigten, die intern für den Datenschutz zuständig sind.

Auch die Rolle der Datenschutzbehörden wandelt sich. Wenn künftig zwei Unternehmen über die Herausgabe von Kund:innendaten streiten, wird es die Datenschutzbehörde sein, die gegebenenfalls anweist, dass der Zugang nach den Voraussetzungen des Data Acts zu gewähren ist.

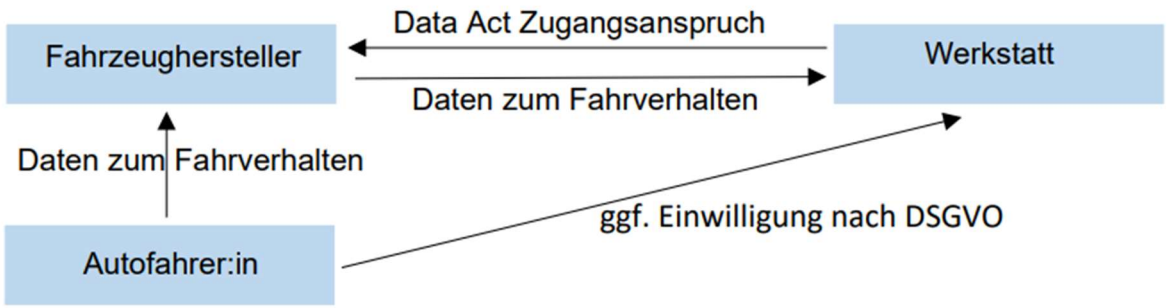
I. Wesentliche Inhalte

Der Data Act zielt darauf ab, bislang bestehende Monopole auf Zugang zu den Daten vernetzter Geräte aufzubrechen. Andere Wirtschaftsteilnehmer:innen sollen ebenfalls die Möglichkeit haben, von den bei der Nutzung entstehenden Daten zu profitieren. Auch den Unternehmen sowie Privatpersonen, die selbst vernetzte Geräte verwenden, soll künftig Zugriff auf die Daten eröffnet werden, die ihre Geräte generieren. Im Fokus steht das sogenannte Internet der Dinge („Internet of Things“), dem zum Beispiel vernetzte Maschinen, Fahrzeuge, Haushaltsgeräte, Fernseher sowie Medizin- und Fitnessgeräte angehören. Bislang ist die Ausgangslage vielfach so, dass die Produkte

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
Ludwig-Erhard-Str. 22, 20459 Hamburg
Tel.: 040/42854-4040 | Fax: 040/42854-4000
E-Mail: mailbox@datenschutz.hamburg.de | Internet: www.datenschutz-hamburg.de

regelmäßig Daten über die Verwendung und zum Beispiel den Verschleiß einzelner Teile an ihre Hersteller senden. So gewinnen beispielsweise Fahrzeughersteller wichtige Rückmeldungen zum Gebrauch ihrer Autos, von denen auch Werkstätten oder Ersatzteilhersteller profitieren könnten. Bislang haben diese jedoch in der Regel keinen freien Zugang. Ebenso geht es den Nutzer:innen. Sowohl Einzelpersonen als auch Unternehmenskunden, die ein internetfähiges Produkt erworben haben, soll der Data Act in die Lage versetzen, selbst zu bestimmen, wem die bei der Nutzung anfallenden Daten offengelegt werden. Diese neuen Einblicksmöglichkeiten werden die Nutzer:innen zunächst selbst in die Lage versetzen, ihr Nutzungsverhalten auszuwerten und eigene Prozesse zu optimieren. Über Lizenzverträge werden Nutzer:innen zudem beispielsweise Werkstätten oder Ersatzteilproduzenten die Auswertung der durch das Gerät erzeugten Daten zur Verfügung stellen können. Der Data Act enthält dabei Bestimmungen über die faire Gestaltung solcher Verträge.

Beispiel: Ein Fahrzeughalter möchte eine Inspektion seines Kfz in einer von ihm ausgesuchten Werkstatt durchführen lassen. Der Data Act gewährleistet, dass die Werkstatt alle Nutzungsdaten erhält, die das Fahrzeug an den Hersteller übermittelt hat. Davon sollen insbesondere die Betreiber profitieren, die keine Vertragswerkstatt des Herstellers sind.



Beispiel: Eine vernetzte elektrische Zahnbürste sendet Daten über die Nutzungsstatistik über das Internet in eine Cloud, damit ihre Benutzer:innen Statistiken in einer App abrufen kann. Der Data Act ermöglicht der Nutzer:in der Zahnbürste, alle Rohdaten einzusehen, auch wenn die App diese nicht oder nur aggregiert anzeigt. Auch Dritte wie zum Beispiel zahnmedizinische Forschungseinrichtungen oder Hersteller von Ersatz-Bürstenköpfen können unter Umständen von den Statistiken profitieren.

Beispiel: Bei Containern in der Frachtschifffahrt sind in der Regel zahlreiche Sensoren integriert, die unter anderem den Standort, die Abnutzung verschiedener Bauteile sowie Vorfälle wie ungewöhnliche Neigungswinkel oder unbefugte Öffnungen erfassen. Per Mobilfunk werden diese Informationen an den Hersteller beziehungsweise Vermieter des

Containers übermittelt. Der Data Act schafft Zugangsmöglichkeiten zum Beispiel für Reedereien, die ihre Routen optimieren möchten oder für Hersteller von Ersatzteilen für abgenutzte Container.

Um diese Ziele zu erreichen, enthält der Data Act zahlreiche neue Rechtspflichten:

- **Datenzugang:** Der Datenzug durch Drittunternehmen ist das Herzstück des Data Acts. Der Zugangsanspruch besteht für alle Arten von Daten – sowohl für personenbezogene Daten als auch für solche ohne Personenbezug. Nach der Zielrichtung des Rechtsakts sind grundsätzlich alle Arten von Daten unter Umständen mit Dritten zu teilen, personenbezogene Daten jedoch nur, wenn das Datenschutzrecht dem nicht entgegensteht. In vielen Fällen wird es aber an einer Rechtsgrundlage für die Herausgabe personenbezogener Unternehmensdaten fehlen. Daher betreffen die Kernpflichten des Data Acts faktisch überwiegend nichtpersonenbezogene Daten. Die Einschätzung, ob ein Personenbezug vorliegt und ob in diesem Fall eine Datenweitergabe mit der DSGVO im Einklang stehen würde, kann nur sinnvoll und verbindlich von dem Personal geprüft und entschieden werden, das im Unternehmen für den Datenschutz zuständig ist.

Beispiel: Die Daten einer vernetzten Zahnbürste geben Aufschluss über den Gesundheitszustand der sie benutzenden Person. Solche Informationen dürfen nur dann mit Dritten geteilt werden, wenn die betroffene Person eingewilligt hat. Kein der Herausgabe entgegenstehender Personenbezug besteht hingegen, wenn die beim Hersteller gespeicherten Daten anonymisiert sind. Dann können zum Beispiel aggregierte Informationen zum Abnutzungsgrad aller Bürstenköpfe an Ersatzteilhersteller gesendet werden.

  Soweit es „relevant und technisch durchführbar“ ist (Art. 3 Abs. 1 DA), ist der Zugang direkt über eine Schnittstelle beziehungsweise ein Kund:innenportal zu gewähren. Andernfalls bedarf es eines Zugangsantrags, der individuell zu bescheiden ist.

- **Notstandsregelungen:** Öffentlichen Stellen sind die Daten vernetzter Geräte offenzulegen im Falle außergewöhnlicher Notwendigkeit wie zum Beispiel Naturkatastrophen und anderen Notständen. Die berechtigten Stellen können im Einzelfall die Herausgabe konkreter Daten verbindlich anordnen, wenn diese zur Bewältigung des Notstands benötigt werden und nicht auf andere Weise effektiv und zeitnah erhoben werden können. Die

Daten sind dann zur Verfügung zu stellen, soweit das Datenschutzrecht dem nicht im Wege steht. Auch Forschungseinrichtungen oder Statistikämter können gegebenenfalls bei außergewöhnlicher Notwendigkeit die Daten erhalten.

Beispiel: Während einer Sturmflut fragt die Innenbehörde Daten aus vernetzten Stromzählern von Wohnhäusern ab, um daraus Rückschlüsse auf den Überflutungsgrad eines Gebietes abzuleiten.

Beispiel: Im Fall eines akuten Mangels an Erdgas während eines starken Winters fragt die zuständige Behörde Daten aus der Füllstandssensorik der deutschen Energiekonzerne oder der Leitungsnetzbetreiber ab.

- **Cloud Switching:** Wirtschaftlich bedeutsam sind die Regelungen zum sogenannten Cloud Switching. Anbieter von Datenverarbeitungsdiensten müssen künftig durch technische Maßnahmen sicherstellen, dass Kund:innen ein einfacher Wechsel zu einem alternativen Anbieter ermöglicht wird. Bisherige Lock-in-Effekte werden dadurch aufgebrochen. Stattdessen sind künftig Prozesse zu etablieren, um mit den Daten von einem Cloud-Anbieter zu einem anderen unkompliziert „umzuziehen“. Auch vertragliche Bindungen, die einem Wechsel entgegenstehen, werden durch den Data Act begrenzt. Die Datensouveränität der Nutzenden wird so durch Interoperabilität gestärkt.

Beispiel: Eine Sportlerin möchte ihre vernetzte Armbanduhr wechseln und dabei die in der Cloud des bisherigen Herstellers gespeicherten Statistiken aus der Vergangenheit weiter fortschreiben.

- **Internationaler Datenverkehr:** Der Data Act unterwirft auch nichtpersonenbezogene Daten territorialen Grenzen. Anbieter von Datenverarbeitungsdiensten haben danach sicherzustellen, dass die betreffenden Daten im europäischen Datenraum verbleiben, wenn eine Drittstaatenübermittlung im Widerspruch zum heimischen Recht stehen würde. Die Anforderungen unterscheiden sich von denen der DSGVO, die im Grundsatz alle Übertragungen personenbezogener Daten in Staaten ohne angemessenes Datenschutzniveau untersagt und nur mit rechtlichen und gegebenenfalls technischen Zusatzmaßnahmen gestattet. Bei nichtpersonenbezogenen Daten ist die Logik umgekehrt: Grundsätzlich ist jede Übertragung in Drittstaaten erlaubt, wird aber im Ausnahmefall Begrenzungen unterworfen.

II. Umsetzungspflichten im Unternehmen

Die Pflichten aus dem Data Act erfordern eine gründliche Vorbereitung in den betreffenden Unternehmen. Auch wenn der Rechtsakt im Kern kein Datenschutzgesetz ist, sind die inhaltlichen Berührungspunkte zur DSGVO unübersehbar. Daher ist es wichtig, die intern mit dem Datenschutz betrauten Beschäftigten mit einzubeziehen. Wesentliche Umsetzungstätigkeiten sind:

- **Anwendungsbereich prüfen**: Nicht alle Unternehmen, die Daten verarbeiten, unterliegen auch Pflichten aus dem Data Act. In den Anwendungsbereich fallen zunächst Stellen, die als Hersteller, Dateninhaber oder Nutzer mit vernetzten Geräten zu tun haben. Spezifische Pflichten treffen zudem Datenverarbeitungsdienste und Cloud-Anbieter. Die behördlichen Zugangsrechte im Fall eines Notstands betreffen potenziell zudem fast alle Unternehmen, unabhängig davon, ob sie vernetzte Geräte verwenden. Für Kleinunternehmen gelten dabei Ausnahmen. Aber auch für Unternehmen, die keinen oder nur minimalen eigenen Pflichten unterliegen, lohnt sich eine Auseinandersetzung mit dem Data Act. Der Rechtsakt kann ihnen gegebenenfalls Chancen bieten, von Daten zu profitieren, die bislang isoliert bei Herstellern liegen.
- **Datenübersicht erstellen**: Wer verpflichtet ist, Zugang zu Informationen zu gewähren, sollte sich zunächst einen Überblick verschaffen, welche Daten vorhanden sind. Das Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DSGVO kann dafür ein erster Anknüpfungspunkt sein. Es enthält jedoch nur Verarbeitungen personenbezogener Daten, während nach dem Data Act auch Daten ohne Personenbezug in den Blick zu nehmen sind. Neben der Vorbereitung auf die Rechtspflichten aus dem Data Act kann die Datenübersicht auch dazu dienen, Potenziale zur optimierten Auswertung des eigenen Datenbestands zu erkennen. Erst die umfassende, zentrale Übersicht lässt erkennen, welche Informationen in den jeweiligen Abteilungen vorhanden sind, die für andere Bereiche von Interesse sein könnten.

> **Beispiel**: Die für Instandsetzungen zuständige Abteilung eines Logistikkonzerns verfügt über Sensordaten von Containern, Eisenbahnwaggons und Lastkraftwagen. Diese Informationen können unter Umständen auch für die Optimierung der Routenplanung hilfreich sein. Dies kann jedoch nur gelingen, wenn die für die Organisation der Lieferwege zuständige Abteilung Kenntnis von der Existenz und dem Format der Sensordaten hat.

- **Personenbezug klären**: Die Frage, ob Dritten Zugang zu Daten zu gewähren ist, kann nur sinnvoll beantwortet werden, wenn bekannt ist, ob die betreffenden Informationen Personenbezug aufweisen oder nicht. Hier ist im Lichte des Data Acts gegebenenfalls eine Neubewertung vorzunehmen. Zwar hat sich die Definition des Personenbezugs nicht geändert. In Zweifelsfällen war es jedoch bislang üblich und sinnvoll, von personenbezogenen Daten auszugehen und sie dem Schutz der DSGVO zu unterwerfen. Künftig muss trennschärfer differenziert werden. Es muss präzise dargelegt werden können, ob ein Datum nichtpersonenbezogen ist und deshalb offengelegt werden muss, oder ob es personenbezogen ist und deshalb gegebenenfalls zurückgehalten werden muss. Insbesondere sind Mischdatensätze zu überprüfen. Gemeinsame Datensätze aus Daten mit und ohne Personenbezug wurden bislang zumeist pauschal als personenbezogene Informationen eingestuft. Künftig bedarf es einer Differenzierung je nach konkretem Datum in dem Mischdatensatz.

- **Geschäftsgeheimnisse kennzeichnen**: Datenschutz ist nicht der einzige mögliche Hinderungsgrund, der einem Datenzugang entgegenstehen kann. So können beispielsweise Zugangsansprüche mit der Begründung abgelehnt werden, dass die betreffenden Daten Geschäftsgeheimnisse sind. Dafür ist es notwendig, darlegen zu können, dass nicht nur der subjektive Wunsch besteht, die Informationen für sich zu behalten. Vielmehr muss ein objektives Geheimhaltungsbedürfnis in dem Sinne bestehen, dass die Verbreitung der Informationen einen Schaden nach sich ziehen würde. Die Einstufung von Daten als Geschäftsgeheimnis sollte in der Datenübersicht entsprechend festgehalten werden.

- **Schnittstellen einrichten**: Vernetzte Produkte sind grundsätzlich so zu konzipieren, dass Nutzer:innen einfach auf die von ihnen generierten Daten zugreifen, sie nutzen und teilen können. Bei der Zugangsgewährung ist auf eine sichere Übertragung zu achten, die nicht von unberechtigten Dritten eingesehen werden kann. Dafür bieten sich entsprechende Schnittstellen und/oder Internetportale mit Kund:innenkonten an. Ein direkter Zugang mittels einer Schnittstelle ist jedoch nicht in jedem Fall zwingend. Es liegt im Ermessen der Hersteller, inwieweit der Direktzugriff „relevant und technisch durchführbar“ im Sinne des Art. 3 Abs. 1 ist. Die Entscheidung des Herstellers muss nachvollziehbar sein und die sorgfältige Begründung sollte dokumentiert werden.

- **Verträge vorbereiten**: Wer künftig zum Abschluss von Lizenzverträgen mit Nutzer:innen und Datenempfänger:innen verpflichtet ist, sollte entsprechende Muster vorbereiten. Dasselbe gilt für ein gegebenenfalls notwendiges Einwilligungsmanagement. Bislang sind

es hauptsächlich die Betroffenen, die Einwilligungen erteilen, damit ihre Daten verarbeitet werden können.

> **Beispiel**: Wenn ein Fahrzeughersteller Sensordaten an einen Ersatzteilhersteller herauszugeben hat, dann sind die Bedingungen dafür in einem Vertrag festzulegen. Insbesondere sollten sich beide Seiten auf einen Preis einigen. Beide Parteien sollten auf solche Verhandlungen vorbereitet sein, indem sie Eckpunkte vorab festlegen und Musterverträge bereithalten. Wenn die Fahrzeugdaten Aufschluss über das Fahrverhalten des Halters oder Nutzers geben, wird der Datenzugang gegebenenfalls eine Einwilligung dieser Personen erfordern. Die Formulierung der Einwilligung sollte nicht dem Endkunden überlassen werden, sondern sollte von den beteiligten Unternehmen entworfen werden.

- **Transparenz**: Der Data Act enthält Informationspflichten unter anderem bei Vertragsschluss über ein vernetztes Produkt. Die vorzubereitenden Texte ähneln den Datenschutzinformationen nach Art. 13 DSGVO, sind aber nicht vollständig deckungsgleich. Sie richten sich gegebenenfalls auch an andere Adressat:innen, weil die Käufer:innen der Geräte nicht zwangsläufig auch die Nutzenden sind. Dennoch ist eine inhaltliche Vereinheitlichung der die Verarbeitungen erklärenden Dokumente nach Data Act und nach der DSGVO sinnvoll.

III. Zusammenspiel aus DSGVO und Data Act

Der Data Act „gilt unbeschadet des (…) Rechts über den Schutz personenbezogener Daten“. Art. 1 Abs. 5 legt damit fest, dass die DSGVO unberührt von den Bestimmungen des Data Acts ist. Die Vorschrift stellt zudem klar, dass im Fall eines Widerspruchs zwischen beiden Rechtsakten die DSGVO Vorrang genießt. Beide Rechtsakte sind europäische Verordnungen gleichen Ranges, aber sie sind mit einer Kollisionsregel zu Gunsten das Datenschutzes versehen. Damit sind in der Anwendung beide Verordnungen möglichst in Einklang zu bringen. Nur dort, wo ein unauflöslicher Widerspruch entsteht, ist im konkreten Fall die betreffende Vorschrift des Data Acts unangewendet zu lassen, um dem Schutz personenbezogener Daten volle Geltung zu verschaffen.
In der Praxis bedeutet dies, dass kein Datenzugang gewährt werden darf, der nicht als zulässige Datenverarbeitung nach der DSGVO gedeckt ist. Relevant ist dies nur für solche Bestimmungen des Data Acts, die sich auf personenbezogene Daten beziehen. Viele Vorschriften des Data Acts gelten

jedoch explizit nur für nichtpersonenbezogene Daten. Ein Beispiel sind die Regelungen zum internationalen Datenverkehr in Art. 31 DA. Unter welchen Voraussetzungen personenbezogene Daten in Drittstaaten versendet werden dürfen, regelt Kap. V. der DSGVO abschließend, während die neuen Einschränkungen des Data Acts ausdrücklich nur für nichtpersonenbezogene Daten gelten. In diesem Themenfeld gibt es daher keine Berührungspunkte zwischen Data Act und DSGVO, sodass beide Rechtsakte parallel zueinander anzuwenden sind.

Das Herzstück des Data Acts betrifft jedoch beide Datenarten: Die Zugangsansprüche für Nutzer:innen und für Dritte gelten sowohl für Daten mit als auch ohne Personenbezug. Ein Datenzugang zu personenbezogenen Daten ist zugleich auch eine Übermittlung beziehungsweise Offenlegung, mithin eine Verarbeitung nach der DSGVO. Nach der Kollisionsregel des Art. 1 Abs. 5 DA ist bei der Gewährung des Zugangs darauf zu achten, dass Datenschutzrechte nicht beeinträchtigt werden. In der Konsequenz bedeutet dies, dass Zugang zu nichtpersonenbezogenen Daten jederzeit zu gewähren ist, wenn die Voraussetzungen vorliegen, Zugang zu personenbezogenen Daten jedoch nur zu gewähren ist, wenn die DSGVO dem nicht entgegensteht. Daten mit Personenbezug dürfen deshalb auch bei Vorliegen der Voraussetzungen aus dem Data Act nur herausgegeben werden, wenn dafür eine Rechtsgrundlage nach Art. 6 DSGVO besteht. Im Fall von besonders schützenswerten Daten im Sinne von Art. 9 Abs. 1 DSGVO muss zusätzlich ein Erlaubnistatbestand nach Abs. 2 gegeben sein. Andernfalls ist der nach dem Data Act gültige Zugangsantrag abzulehnen beziehungsweise keine Schnittstelle freizuschalten.

> **Beispiel**: Die Laufuhr einer Sportlerin erhebt Daten über ihren Fitnesszustand. Der Einrichtung einer Schnittstelle für die Sportlerin, mit der sie ihre eigenen Laufstatistiken in einer App abrufen kann, steht das Datenschutzrecht nicht entgegen. Daher verfügt die Läuferin über einen entsprechenden Zugangsanspruch aus dem Data Act.

Ist die Stelle, die den Zugang für sich oder einen Dritten beantragt, zugleich die betroffene Person im Sinne von Art. 4 Nr. 1 DSGVO, so wird eine Rechtsgrundlage nach Art. 6 DSGVO in der Regel nicht zum Problem. Die betroffene Person kann dann in die Datenübermittlung einwilligen. Je nach seiner konkreten Formulierung kann auch der Antrag selbst als konkludente Einwilligung zu würdigen sein. Möglich sind auch Verträge zwischen der betroffenen Person und einem Dritten, die zusammen mit Art. 6 Abs. 1 lit. b) DSGVO die Rechtsgrundlage für die Offenlegung bilden.
Ist die den Zugang beantragende Stelle nicht zugleich die betroffene Person im Sinne des Datenschutzrechts, ist im Einzelfall ein mögliches überwiegendes berechtigtes Interesse nach Art. 6 Abs. 1 lit. f) DSGVO oder auch ein anwendbarer Vertrag nach lit. b) als mögliche Rechtsgrundlage

zu prüfen. Alternativ ist zu erwarten, dass Unternehmen, die personenbezogene Daten nutzen möchten, künftig die Betroffenen auffordern, eine Einwilligung zu auszusprechen.

Beispiel: Möchten andere Stellen wie zum Beispiel Fitnessstudios oder Krankenversicherungen Daten der Laufuhr der Sportlerin abrufen, benötigen sie dafür eine Rechtsgrundlage nach der DSGVO. Hier gilt es zu beachten, dass Informationen über den Fitnesszustand der Sportlerin Gesundheitsdaten nach Art. 9 Abs. 1 DSGVO sind. Diese dürfen in der Regel nur offengelegt werden, wenn die Sportlerin darin eingewilligt hat. Entsprechende Schnittstellen zu den IT-Systemen Dritter sind daher erst freizuschalten, wenn gewährleistet ist, dass die Voraussetzungen für die Datenübermittlung vorliegen.

Beispiel: Ein Automobilclub möchte zur Optimierung seines Reparaturdienstes Nutzungsdaten von Fahrzeugen anfordern, die bislang nur bei den jeweiligen Herstellern vorliegen. Um den Zugangsanspruch in Einklang mit dem Datenschutzrecht zu bringen, hat der Automobilclub die Möglichkeit, seine Mitglieder aufzufordern, vorformulierte Einwilligungen gegenüber den jeweiligen Herstellern zu erteilen. Der Club kann die Einwilligungserklärungen zum einen selbst einsammeln und seinem Zugangsantrag an die Hersteller beifügen. Alternativ kann der Club die Mitglieder auffordern, ihre Einwilligungen selbst an den jeweiligen Fahrzeughersteller zu senden.

Der Zugangsanspruch aus dem Data Act überschneidet sich inhaltlich stark mit dem Recht auf Datenübertragbarkeit aus Art. 20 DSGVO, wenn die Nutzer:in zugleich Betroffene:r ist. Inhaltlich geht der Anspruch aus dem Data Act weiter, weil er auch nichtpersonenbezogene Daten umfasst. Wenn Zugangsanträge gestellt werden, weil keine Schnittstelle für den direkten Zugang eingerichtet ist, muss durch Auslegung ermittelt werden, welcher der beiden Anträge gestellt wurde. Im Zweifel ist davon auszugehen, dass die Anträge aus DSGVO und Data Act parallel geltend gemacht wurden, wenn keine explizite Eingrenzung erfolgt ist. Dies hat die Konsequenz, dass mitunter dieselben Daten aus unterschiedlichen Gesetzen herausverlangt werden können. Fallen die Aufsichtsbehörden nach dem Data Act und der DSGVO auseinander, kann derselbe Sachverhalt dann bei beiden Behörden angezeigt und von beiden Behörden verfolgt werden.

Neben der Rechtmäßigkeit eines Datenzugangs überschneiden sich beide Rechtsakte in Fragen der Datensicherheit. Sowohl Data Act als auch DSGVO verpflichten die beteiligten Akteur:innen, den Datenaustausch sicher zu gestalten und auch die empfangenden Daten mittels technisch-organisatorischer Maßnahmen vor dem Zugriff durch Unbefugte zu sichern. Diese Vorgabe aus Art. 32 DSGVO weist starke Ähnlichkeit mit Art. 4 Abs. 6, Art. 5, Art. 17 Abs. 1 lit. g) und Art. 19 Abs.

1 lit. b) DA auf. Diese Regelungen enthalten für jeweils spezifische Konstellationen die Vorgabe, technisch-organisatorische Maßnahmen zur Gewährleistung der Vertraulichkeit einzurichten. Welche dies konkret sind und wie weit das herzustellende Schutzniveau reicht, wird in beiden Rechtsakten nach einem risikobasierten Ansatz anhand der Schutzwürdigkeit der Daten, der Wahrscheinlichkeit eines Angriffs und den Umständen des Einzelfalls bemessen. DSGVO und Data Act geben hier dasselbe Ziel und dieselbe Methodik vor. Daher empfiehlt sich eine Umsetzung mittels einheitlicher Schutzmaßnahmen unabhängig vom Personenbezug der betreffenden Daten.

IV. Behördliche Aufsicht

Die wesentlichen Inhalte des Data Acts sind in Form von zivilrechtlichen Ansprüchen auf Datenzugang ausgestaltet, die durch Lizenzverträge konkretisiert werden können. Auch die Rechtsdurchsetzung ist damit in erster Linie mit Fokus auf die Verfolgung privater Ansprüche auf dem Zivilrechtsweg angelegt. Der Data Act sieht jedoch ergänzend auch eine aufsichtsbehördliche Struktur vor.

1. Zweigeteilte Aufsicht

Die Aufsicht ist nach Art. 37 DA zweigeteilt. Zunächst hat jeder Mitgliedstaat eine „Haupt-Aufsichtsbehörde“ für alle Konstellationen zu benennen, die nicht den Schutz personenbezogener Daten betreffen. Soweit hingegen ein Aufsichtsfall personenbezogene Daten betrifft, sind nach Art. 37 Abs. 3 DA automatisch die für die Überwachung der DSGVO zuständigen Behörden auch Aufsichtsbehörde nach dem Data Act. Nur im ersten Fall gibt es einen Umsetzungsspielraum der Mitgliedstaaten. Im zweiten Fall gibt es nichts umzusetzen, weil das Unionsrecht unmissverständlich die nach der DSGVO eingesetzten Datenschutzbehörden benennt. Die gesetzgeberische Intention ist nachvollziehbar. Fragestellungen, ob nach dem Data Act Zugang zu einem personenbezogenen Datum zu gewähren ist, werden vor allem daran zu messen sein, ob die Voraussetzungen der DSGVO dem entgegenstehen oder nicht. Dies kann nur verbindlich von der Behörde entschieden werden, die ohnehin für die Aufsicht über die DSGVO zuständig ist. Daher hat sich der Unionsgesetzgeber in Fällen mit personenbezogenen Daten für einen zwingenden Gleichlauf mit der Behördenstruktur nach der DSGVO entschieden.

2. Datenschutz-Vorschriften im Data Act

Die Datenschutzbehörden sind nach Art. 37 Abs. 3 UAbs. 1 DA „bezüglich des Schutzes personenbezogener Daten auch für die Überwachung der Anwendung der vorliegenden Verordnung

zuständig.“ Nicht mit letzter Klarheit bestimmt die Vorschrift, welche Fallgruppen des Data Acts den „Schutz personenbezogener Daten“ zum Gegenstand haben. Bei enger Auslegung könnte die Zuständigkeitsvariante auf solche Regelungen beschränkt sein, die explizit den „Schutz“ zum Gegenstand haben, also nicht die Zugänglichmachung, sondern die Beschränkung der Verfügbarkeit. Eine solche enge Lesart würde jedoch das Ziel des Gesetzgebers konterkarieren, bei Zugangsanträgen aus einer Hand zu beurteilen, ob Anforderungen der DSGVO ihnen entgegenstehen. Nach vorzugswürdiger Auslegung sind die Datenschutzbehörden deshalb immer dann zuständig, wenn personenbezogene Daten in einem Sachverhalt betroffen sind. Insbesondere die Gewährung und Ablehnung des Zugangs zu personenbezogenen Daten ist damit durch die Datenschutzbehörden zu gewährleisten.

Damit besteht eine Zuständigkeit je nach Fallkonstellation für alle Vorschriften des Data Acts, die nicht auf nichtpersonenbezogene Daten beschränkt sind. Die Bestimmungen des Data Acts, die jedenfalls auch personenbezogene Daten zum Gegenstand haben, sind insbesondere

Art. 3 DA: Zugänglichmachung von Produktdaten vernetzter Produkte
Art. 4 DA: Zugang zu und Nutzung von Produktdaten bei vernetzten Produkten
Art. 5 DA: Weitergabe von Daten an Dritte
Art. 6 DA: Verarbeitung personenbezogener Daten durch Dritte
Art. 8 DA: Obligatorische Verträge zwischen Dateninhaber und Datenempfänger
Art. 9 DA: Gegenleistung für die Bereitstellung von Daten
Art. 11 DA: Technische Schutzmaßnahmen
Art. 13 DA: Missbräuchliche Vertragsklauseln
Art. 14 f. DA: Datenbereitstellung wegen außergewöhnlicher Notwendigkeit
Art. 19 f. DA: Pflichten öffentlicher Stellen, die Daten erhalten haben
Art. 23 ff. DA: Wechsel des Anbieters von Datenverarbeitungsdiensten
Art. 33 ff. DA: Interoperabilität/Datenräume

3. Aufgaben und Befugnisse der Aufsichtsbehörde

Die Aufgaben und Befugnisse der Datenschutzbehörde sind im Data Act nicht explizit aufgezählt, sondern werden durch einen Verweis auf die DSGVO geschaffen. In Art. 37 Abs. 3 Satz 2 DA heißt es: „Die Kapitel VI und VII der Verordnung (EU) 2016/679 finden sinngemäß Anwendung.“ Die in Bezug genommenen beiden Kapitel enthalten die folgenden Inhalte:

- Kap. VI DSGVO: Unabhängige Aufsichtsbehörden, darin die Befugnisse (Art. 51-59 DSGVO) und Aufgaben (Art. 57 DSGVO).
- Kap. VII DSGVO: Zusammenarbeit und Kohärenz (Art. 60-76 DSGVO)

Die dort enthaltenen Aufgaben und Befugnisse sind damit auch hinsichtlich etwaiger Verletzungen des Data Acts im Zusammenhang mit personenbezogenen Daten auszuüben. Der Passus „sinngemäß“ schränkt den Verweis dahingehend ein, dass solche Befugnisse, die im Zusammenhang mit dem Data Act keinen Sinn ergeben, nicht gemeint sind (zum Beispiel Art. 58 Abs. 2 lit. h DSGVO zur Rücknahme von Zertifizierungen, die der Data Act nicht vorsieht).
Wichtige Aufgaben und Befugnisse der Datenschutzbehörde in ihrer Eigenschaft als Aufsichtsbehörde nach dem Data Act sind unter anderem die folgenden, über den Verweis inkorporierten Bestimmungen der DSGVO:

- Untersuchungsbefugnisse (Art. 58 Abs. 1 DSGVO)
- Warnungen und Verwarnungen (Art. 58 Abs. 2 lit. a, b DSGVO)
- Anordnungen (Art. 58 Abs. 2 lit. c-g, j DSGVO)
- Geldbußen (Art. 58 Abs. 2 lit. i DSGVO; siehe dazu unten)
- Aufgaben wie Sensibilisierung der Öffentlichkeit (Art. 57 Abs. 1 lit. b DSGVO), Beratung öffentlicher Stellen (lit. c), Sensibilisierung der von der Verordnung verpflichteten Stellen (lit. d sinngemäß) usw.
- Eigenständige Entgegennahme und Bearbeitung von Beschwerden (Art. 57 Abs. 1 lit. f DSGVO in Verbindung mit Art. 38 DA)
- Erstellung eines Tätigkeitsberichts (Art. 59 DSGVO)
- Kooperationsverfahren unter den Mitgliedern des Europäischen Datenschutzausschusses (Art. 60 ff. DSGVO)

Die Datenschutzbehörden werden damit ab September 2025 neben Beschwerden nach der DSGVO auch Beschwerden nach dem Data Act entgegennehmen. In analoger Anwendung der Verfahrensvorschriften der DSGVO werden sie gemeldeten Verstößen gegen den Data Act nachgehen und dabei Untersuchungs- und Abhilfebefugnisse ausüben. Die Bearbeitung der Data-Act-Fälle sollte dabei primär im Zusammenspiel den Abteilungen für Industrie und für Informationsfreiheit erfolgen. Die Federführung der Referent:innen für Datenschutz in der Industrie ist essenziell für die einheitliche Beurteilung relevanter Fragen zum Beispiel des Personenbezugs von Daten und der Rechtmäßigkeit von Übermittlungen. Zudem werden Zugangsanträge oftmals gleichzeitig als Auskunftsanträge nach Art. 15 DSGVO einzustufen sein – eine strikte Trennung der internen Zuständigkeit stünde dem entgegen. In die Fallbearbeitung sind zudem die Abteilungen für Informationsfreiheit einzubeziehen, soweit die jeweilige Datenschutzbehörde dafür mit zuständig ist.
Die Transparenzgesetze der Länder weisen unübersehbare Parallelen zum Data Act auf. Beide Rechtsakte zielen darauf ab, Daten auf Antrag offenzulegen, die bis dahin der Öffentlichkeit nicht zur Verfügung standen. Dem jeweiligen Zugangsantrag stehen gegebenenfalls Datenschutzrechte

oder Geschäftsgeheimnisse entgegen – genau zu diesen Fragestellungen haben die Informationsfreiheitsbeauftragten eine langjährige Expertise entwickelt.

Nicht Teil des Verweises aus dem Data Act in die Befugnisnormen des Datenschutzrechts ist Art. 83 DSGVO zur Verhängung von Bußgeldern. Die Befugnis, Geldbußen zu verhängen, wird jedoch über Art. 58 Abs. 2 lit. i DSGVO aus der DSGVO in den Data Act „hineingezogen“. Diese Befugnisnorm ist allerdings noch kein Bußgeldtatbestand. Die Sanktionstatbestände sind nach Art. 40 DA von den Mitgliedstaaten zu schaffen. Das zu erwartende deutsche Data-Act-Durchführungsgesetz muss deshalb entsprechende Vorschriften enthalten, die auch die Datenschutzbehörden dazu befähigen, wirksame, verhältnismäßige und abschreckende Sanktionen zu erlassen, die den Anforderungen des Art. 40 Abs. 3 a-f DA gerecht werden.

Beispiel: Der Nutzer einer vernetzten Zahnbürste verlangt vom Hersteller die Herausgabe aller Daten, die von der Zahnbürste aus in eine Cloud eingespeist wurden. Die Datenschutzbehörde kann den Händler verbindlich anweisen, diese Informationen bereitzustellen, soweit sie beim Hersteller personenbezogen vorliegen, also zum Beispiel mit einem Benutzer:innenkonto verknüpft sind. Speichert der Hersteller lediglich aggregierte Daten, die nicht auf ein bestimmtes Gerät bezogen sind, können etwaige Zugangsansprüche auf solche statistischen Informationen nur durch die Aufsichtsbehörde nach Art. 37 Abs. 1 DA verfolgt werden (gegebenenfalls BNetzA).

Beispiel: Der Anbieter eines Navigationssystems verlangt von einem Logistikunternehmen die Herausgabe von GPS-Daten der LKW-Flotte. Da es sich nicht um privat genutzte Fahrzeuge handelt, ist die Frage entscheidend, ob die angefragten Daten Rückschlüsse auf die Beschäftigten zulassen. Relevant für die Einstufung ist die Unterscheidung, ob der Betreiber des Navigationssystems über rechtliche und tatsächliche Möglichkeiten verfügt, zu ermitteln, welche Einzelperson den zum jeweiligen Datensatz gehörenden LKW gesteuert hat. Ist diese Möglichkeit gegeben, überwacht die Datenschutzbehörde die Rechtmäßigkeit der Gewährung oder Ablehnung des Datenzugangs. Fehlt es an einer Rechtsgrundlage für die Datenübermittlung, untersagt sie gegebenenfalls den Zugang. Besteht eine Rechtsgrundlage, zum Beispiel aufgrund überwiegender berechtigter Interessen oder aufgrund einer Einwilligung der fahrzeugführenden Person, ordnet sie gegebenenfalls die Zugangsgewährung an.

Beispiel: Ein Automobilclub fordert seine Mitglieder auf, Datenzugang beim jeweiligen Fahrzeughersteller zu beantragen und die Daten dem Club zur Verfügung zu stellen. Der

Automobilclub stellt entsprechende Antrags- und Einwilligungsformulare zur Verfügung. Die Datenschutzbehörde des Bundeslands am Sitz des Fahrzeugherstellers überprüft die Gültigkeit der Einwilligung und sonstigen Zugangsvoraussetzungen und ordnet gegebenenfalls die Zugangsgewährung an.

Beispiel: Ein Unternehmen wechselt zu einem neuen Cloud-Anbieter. Die in der bisherigen Cloud gespeicherte Kund:innendatenbank soll auf den Onlinespeicherplatz des neuen Anbieters transferiert werden. Die Datenschutzbehörde überprüft sowohl die Voraussetzungen nach der DSGVO insbesondere auf korrekte Umsetzung des Auftragsverarbeitungsverhältnisses als auch die reibungslose Gewährleistung des Umstiegs durch den bisherigen Cloud-Anbieter. Sind Cloud-Nutzer (als verantwortliche Stelle im Sinne der DSGVO) und Cloud-Anbieter (als Verpflichteter nach dem Data Act) in unterschiedlichen Bundesländern oder Mitgliedstaaten angesiedelt, arbeiten die beiden jeweils für einen Teilaspekt örtlich zuständigen Datenschutzbehörden nach den Kooperationsmechanismen der DSGVO vertrauensvoll zusammen.

4. Zuständige Aufsichtsbehörden in Deutschland

Wer Aufsicht für den „Hauptteil“ in Bezug auf nichtpersonenbezogene Daten wird, ist in Deutschland noch nicht entschieden. Die übrigen EU-Mitgliedstaaten haben überwiegend ihre Datenschutzbehörden auch für diese Konstellation benannt, um eine möglichst einheitliche Aufsicht aus einer Hand zu gewährleisten. Dies wäre für die Betroffenen, Nutzer:innen und verpflichteten Stellen die einfachste Lösung.

Ein an 05. Februar 2025 erstellter Referentenentwurf der scheidenden Bundesregierung für ein Data-Act-Durchführungsgesetz schlägt als Aufsichtsbehörde für nichtpersonenbezogene Konstellationen die Bundesnetzagentur (BNetzA) vor. Soweit der Schutz personenbezogener Daten vom Data Act umfasst ist, soll die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) die alleinige Aufsichtsbehörde sein. Der vom Unionsrecht vorgegebene Gleichlauf mit den jeweils zuständigen Datenschutzbehörden wird damit nicht erzielt. In den meisten Konstellationen ist die jeweilige Landesdatenschutzbehörde zuständig für die Überwachung der Einhaltung der DSGVO. Umsetzende Stellen würden sich in dem Szenario künftig sowohl mit der Landes- als auch der Bundesdatenschutzaufsicht über ihre Datenverarbeitungen abstimmen müssen – ein klarer Widerspruch zu Art. 37 Abs. 3 DA. Die BfDI würde nach dem Gesetzesentwurf allerdings auch nicht, wie im Data Act vorgesehen, eine vollwertige Aufsichtsbehörde werden, die die ihr in dem Fall unionsrechtlich zugewiesenen Aufgaben und Befugnisse ausübt. Die Behörde ist

als zuarbeitende Stelle für die Bundesnetzagentur vorgesehen. Die BNetzA soll auch hinsichtlich der Datenschutzvorschriften im Data Act eine einheitliche Entscheidung unter eigenem Briefkopf treffen, in die die Vorarbeiten der BfDI lediglich einfließen sollen.

Ab September 2025 ist der Data Act umzusetzen. Dieses Datum bindet auch die mitgliedstaatliche Behördenstruktur. Ob es unter der gegenwärtigen bundespolitischen Ausgangslage gelingt, ein deutsches Umsetzungsgesetz bis dahin zu verabschieden, ist ungewiss. Wird bis zum September kein solches Gesetz erlassen, sind die Landesdatenschutzbehörden dann automatisch Kraft Unionsrechts die Aufsichtsbehörden für die Vorschriften und Konstellationen des Data Acts hinsichtlich des Schutzes personenbezogener Daten. Eine Aufsicht für Fallgestaltungen nichtpersonenbezogener Daten gibt es dann zunächst nicht. Die Datenschutzbehörden würden dann zeitweise die einzigen Aufsichtsbehörden für den Data Act sein. Falls rechtzeitig ein Umsetzungsgesetz erlassen werden kann, ist es ungewiss, ob es dem derzeitigen Referentenentwurf entsprechen wird. Zum einen europarechtliche Bedenken in Kombination mit verfassungsrechtlichen Schwierigkeiten einer Bundesaufsicht auch über öffentliche Stellen der Länder dagegen, das Gesetz in der aktuell vorgeschlagenen Version zu beschließen. Zum anderen ist es zweifelhaft, dass der in dem Entwurf angelegte Versuch einer einheitlichen Aufsicht durch die BNetzA den gewünschten Effekt erzielt. Wenn sich datenverarbeitende Stellen künftig für eine verbindliche Auskunft gleichzeitig sowohl an ihre Landesdatenschutzbehörde als auch an BNetzA und BfDI werden wenden müssen, wird der Bürokratieaufwand nicht abgesenkt, sondern stark erhöht.

Die Landesdatenschutzbehörden müssen sich derzeit darauf vorbereiten, ab September die ihnen in Art. 37 Abs. 3 DA zugewiesene Aufsichtsaufgabe wahrzunehmen. Unter dem gegenwärtigen Zeitdruck ist es nicht angezeigt, darauf zu warten, ob und wie der Bundesgesetzgeber die unionsrechtlichen Vorgaben an die Aufsicht modifiziert.