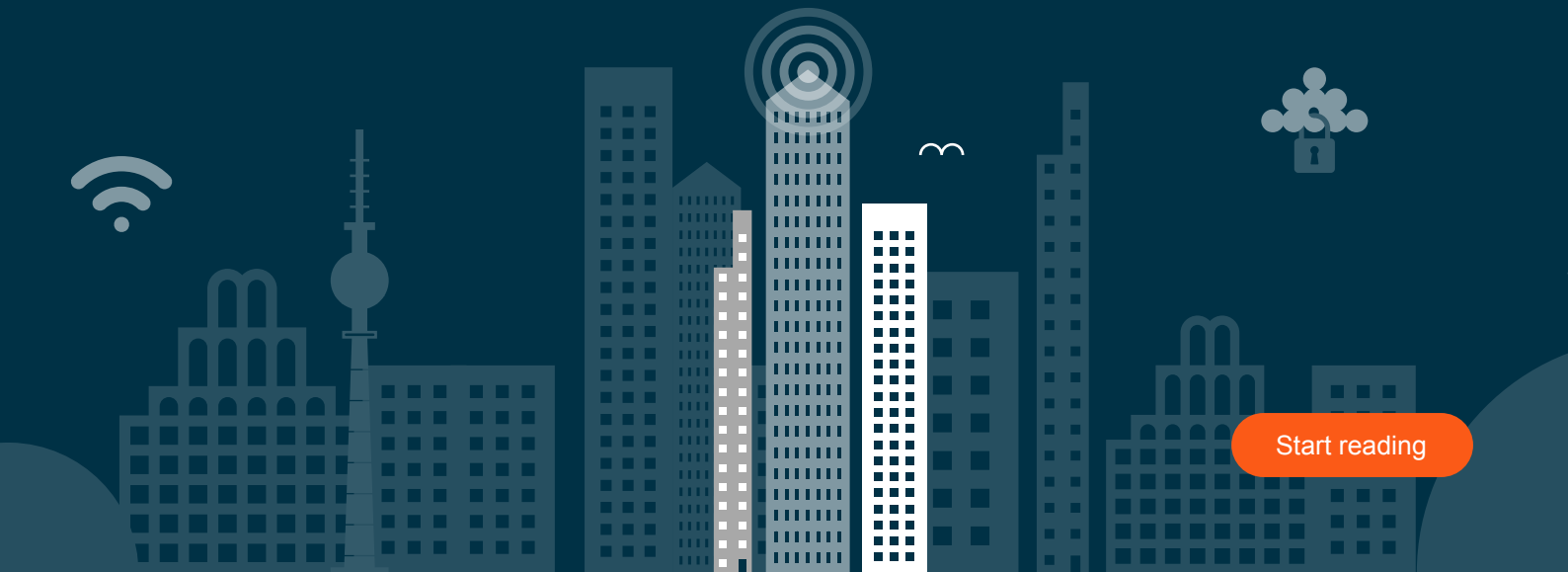
Osborne Clarke

Data Act 360°

Ihre Roadmap zur Compliance



Start reading

Contents

1. Was regelt der Data Act überhaupt?

Am 11. Januar 2024 ist die europäische Datenverordnung (Data Act – Verordnung (EU) 2023/2854) in Kraft getreten, die grundsätzlich seit dem 12. September 2025 zur Anwendung gekommen ist. Deshalb ist es für Unternehmen höchste Zeit, zu prüfen, ob sie von den neuen Regelungen des Data Act betroffen sind und wie sie diese umsetzen können.

Warum ist das wichtig? Verstöße gegen den Data Act werden durch die EU-Mitgliedsstaaten sanktioniert, wobei die Art der Sanktionen (einschließlich der Höhe etwaiger Bußgelder) nicht direkt im Data Act geregelt ist, sondern von den einzelnen Mitgliedsstaaten im nationalen Recht festgelegt wird.

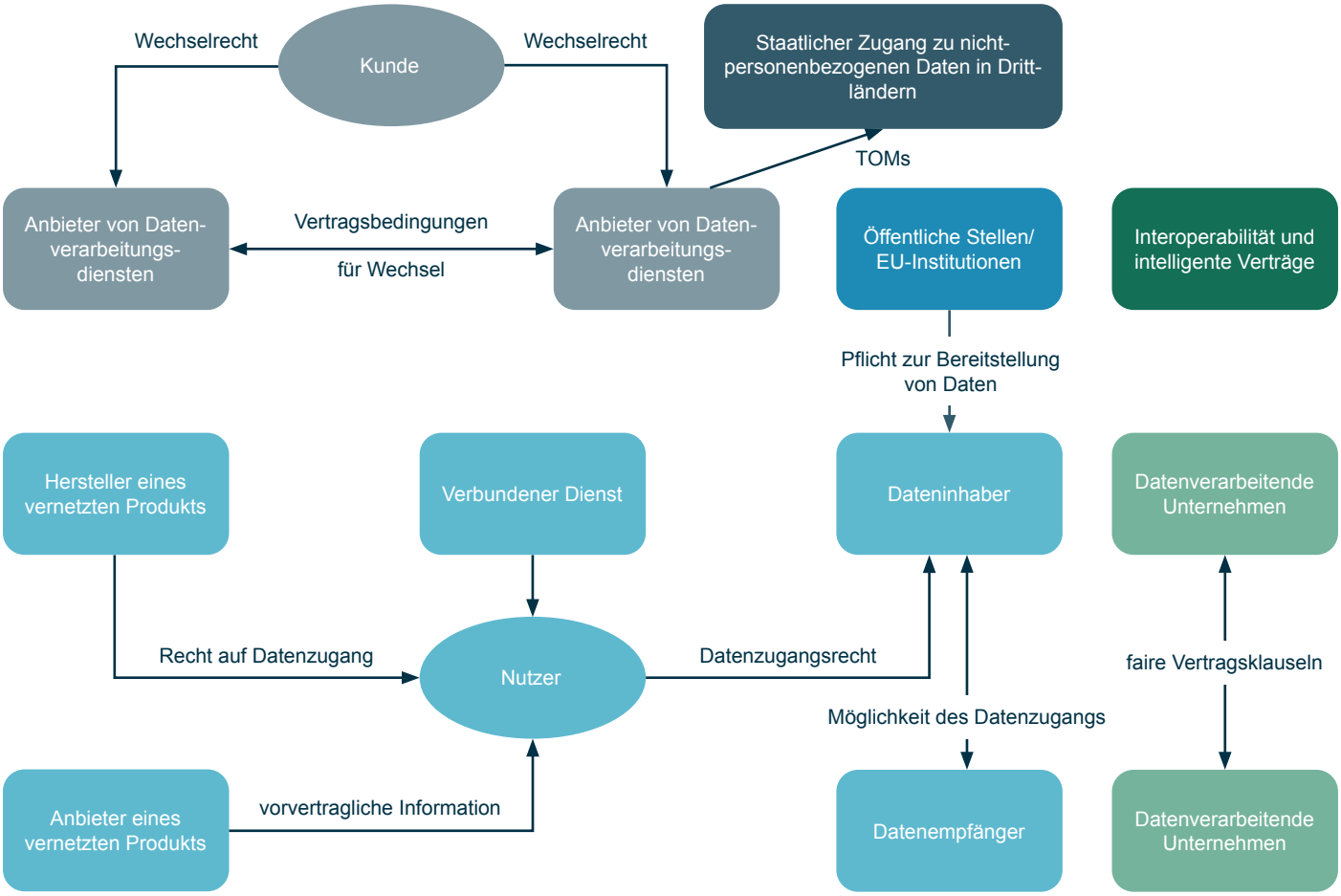
Der Data Act umfasst ein Potpourri rechtlicher Vorschriften, die für Unternehmen unterschiedlich relevant sein können. In unserer Artikel-Reihe zum Data Act möchten wir diese Regelungen vorstellen.

Teil 1 unserer Reihe bietet einen Überblick über die Regelungskomplexe des Data Act. In den folgenden Beiträgen stellen wir die einzelnen Regelungskomplexe im Detail vor, analysieren die Auswirkungen auf Unternehmen und zeigen Umsetzungsmaßnahmen auf.

Welche Regelungskomplexe enthält der Data Act?

Der Data Act beinhaltet verschiedene Regelungskomplexe, die je nach Geschäftsmodell für Unternehmen unterschiedlich relevant sind. Die folgende Übersicht illustriert das:

Überblick zu den Regelungen des Data Act



- Recht auf Datenzugang, Art. 3 ff. DA
- Wechsel von Diensten, Art. 23 ff. DA
- Staatlicher Zugang in Drittländern, Art. 32 DA
- faire Vertragsbedingungen, Art. 13 DA
- öffentliche Stellen/EU-Institutionen, Art. 14 ff. DA
- Interoperabilität und intelligente Verträge, Art. 33 und 36 DA

Data Act Kapitel II und III: Recht auf Datenzugang

Anbieter von vernetzten Produkten und damit verbundenen Diensten sind gemäß Art. 3 ff. Data Act verpflichtet, auf Verlangen des Nutzers diejenigen Daten zugänglich zu machen, die durch die Nutzung eines vernetzten Produktes oder verbundenen Dienstes generiert wurden. Was gehört beispielsweise dazu?

- Vernetzte Produkte sind mit dem Internet verbundene Produkte, etwa Smart Cars, bestimmte Medizinprodukte, Smart Meter, Smart TVs, Smart Watches oder smarte Küchengeräte.

- Verbundene Dienste sind z. B. Apps, mit denen sich ein vernetztes Produkt steuern lässt, wie eine App zur Steuerung von Smart-Home-Geräten.

Auf Verlangen des Nutzers müssen Anbieter die durch das vernetzte Produkt oder den verbundenen Dienst generierten Daten sowohl dem Nutzer selbst als auch einem vom Nutzer benannten Dritten zugänglich machen. Für den Nutzer ist dieser Datenzugang kostenlos, gegenüber dem Dritten kann der Anbieter hingegen ein angemessenes Entgelt verlangen.

Diese Regelung soll es Nutzer ermöglichen, Folgemarkt-Dienste (sog. After Market Services), Nebendienste und sonstige Dienste, insbesondere im Zusammenhang mit dem vernetzten Produkt oder dem verbundenen Dienst, zu nutzen, die von Dritten (eventuell kostengünstiger) angeboten werden. Außerdem soll die Nutzungsmöglichkeit der generierten Daten durch Dritte die Innovation und Entwicklung neuer, bedarfsgerechter Dienste oder Produkte fördern. Versicherungen könnten beispielsweise ihre Prämien entsprechend den Risken bei der Nutzung der Produkte staffeln.

Die Nutzung der generierten Daten durch Dritte unterliegt jedoch Beschränkungen. Insbesondere dürfen die Dritten diese Daten nicht verwenden, um ein Produkt zu entwickeln, das mit dem vernetzten Produkt im Wettbewerb steht. Auch der Versuch, dadurch Einblicke in die wirtschaftliche Lage, die Vermögenswerte und die Produktionsmethoden des Anbieters oder die Nutzung durch den Anbieter zu gewinnen, ist verboten. Zudem kann das Datenschutzrecht das Recht auf Datenzugang beschränken, weil die Bestimmungen der DS-GVO vom Data Act unberührt bleiben.

Data Act Kapitel IV: Verbot missbräuchlicher Vertragsklauseln

Wenn ein Anbieter nach Art. 5 Data Act auf Verlangen eines Nutzers einem Dritten Zugriff auf generierte Daten gewähren muss, sollte der Anbieter mit dem Dritten einen Vertrag zur Regelung des Datenzugangs und der Datennutzung abschließen. So kann der Anbieter seine Interessen, insbesondere bezüglich des Schutzes von Geschäftsgeheimnissen oder bezüglich eines Entgelts, schützen. Die Klauseln eines solchen Vertrages, soweit sie nicht verhandelt werden, dürfen nach Maßgabe von Art. 13 Data Act nicht missbräuchlich sein, ansonsten sind sie für den anderen Vertragsteil nicht bindend.

Data Act Kapitel V: Datenbereitstellung an öffentliche Stellen und EU-Institutionen

Neben der Pflicht zur Datenzugänglichmachung an Nutzer und Dritte können laut Art. 14 ff. Data Act auch öffentliche Stellen und EU-Institutionen vom Anbieter (oder anderen Dateninhabern) die Bereitstellung von Daten verlangen, wenn eine „außergewöhnliche Notwendigkeit“ besteht. Die Regelungen entstanden aufgrund der Erfahrungen aus der Covid-Pandemie. Sie haben gezeigt, dass der Zugriff der öffentlichen Stellen und EU-Institutionen auf gewisse Daten relevant sein kann für die Beurteilung und Ergreifung von angemessenen Maßnahmen.

Data Act Kapitel VI: „Cloud Switching“

Sowohl B2B- als auch B2C-Kunden sollen nach Art. 23 ff. Data Act kurzfristig und ohne Hindernisse von einem Cloud-Anbieter zum anderen oder zu einer On-premises-Lösung wechseln können. Zweck dieses Regelungskomplexes ist es, den Wettbewerb zu fördern und Marktzutrittsschranken für neue Anbieter zu senken, besonders durch die Beseitigung von vertraglichen Lock-In-Effekten.

Diese Regelungen gelten aber nicht nur für die klassischen Cloud-Dienste, sondern auch für andere Datenverarbeitungsdienste, wie Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS), Storage-as-a-Service und Database-as-a-Service (DaaS). Anbieter sind verpflichtet, die für den Wechsel erforderlichen Unterstützungsleistungen zu erbringen, insbesondere beim Exportieren und Übertragen von Daten und digitalen Vermögenswerten (digital assets). Die diesbezüglichen Rechte von Kunden sind in einem schriftlichen Vertrag zwischen Anbieter und Kunde festzulegen. Ab dem 12. Januar 2027 müssen Anbieter diese Unterstützungsleistungen kostenlos erbringen.

Data Act Kapitel VII: Herausgabe von nicht-personenbezogenen Daten an ausländische Behörden

In Anlehnung an Kapitel V der DS-GVO, insbesondere Art. 48 DS-GVO zur Übermittlung personenbezogener Daten an Gerichte und Behörden in Drittländern, enthält Art. 32 Data Act Anforderungen für Anbieter, wenn sie nicht-personenbezogene Daten, die in der EU gespeichert sind, an ein Gericht oder eine Behörde außerhalb der EU übermitteln (sollen). Diese Anforderungen gelten auch dann, wenn das ausländische Gericht oder die ausländische Behörde eine Entscheidung erlassen hat, die den Anbieter dazu auffordert, solche nicht-personenbezogenen Daten zu übermitteln oder zugänglich zu machen.

Data Act Kapitel VIII: Interoperabilität bei europäischen Datenräumen

Besondere Anforderungen zur Interoperabilität gelten nach Art. 33 ff. Data Act für die Nutzung europäischer Datenräume. Interoperabilität bedeutet die Fähigkeit von zwei oder mehr Datenräumen, Daten auszutauschen und zu nutzen, um ihre Funktionen auszuführen (Art. 2 Nr. 40 Data Act). Teilnehmer an europäischen Datenräumen müssen künftig bestimmte Informationen offenlegen. Dazu zählen etwa Datensatzinhalte, Datenstrukturen und Angaben dazu, welche technischen Mittel für den Datenzugang und deren Übermittlung genutzt werden. Ziel und Zweck der Regelungen ist es, dass Daten zwischen verschiedenen Datenräumen zur Innovationsförderung weitergegeben und ausgetauscht werden können.

Kapitel VIII: Smart Contracts

Künftig gelten zudem besondere Vorgaben für den Einsatz intelligenter Verträge. Intelligente Verträge bezeichnen Computerprogramme, die für die automatisierte Ausführung einer Vereinbarung oder eines Teils davon verwendet werden (Art. 2 Nr. 39 Data Act).

Der Data Act sieht vor, dass intelligente Verträge künftig bestimmte Anforderungen erfüllen müssen, wenn sie für die automatisierte Ausführung von Datenweitergabe- und Datenbereitstellungsvereinbarungen eingesetzt werden. In diesem Fall müssen sie nach Art. 36 Data Act so robust gestaltet sein, dass Funktionsfehler vermieden werden und eine Zugangskontrolle möglich ist, um Manipulationen durch Dritte vermeiden zu können. Anbieter von intelligenten Verträgen müssen die Einhaltung der neuen Anforderungen künftig durch eine EU-Konformitätserklärung nachweisen.

Tiefergehende Einblicke in die verschiedenen Regelungskomplexe des Data Acts, einschließlich datenschutzrechtlicher Erwägungen und Aspekte zum Schutz von Geschäftsgeheimnissen, werden wir in nachfolgenden Teilen dieser Reihe geben.

2. Geltendmachung von Ansprüchen unter dem Data Act

Für zahlreiche Unternehmen lässt der Data Act weitreichende Konsequenzen erwarten. Denn die Vorgaben des Data Act treffen – anders als beispielsweise beim Digital Markets Act – nicht nur ausgewählte Unternehmen, sondern jeden Hersteller oder Anbieter von vernetzten Produkten und verbundenen Diensten. Auch dürften Unternehmen wechselseitig auf Basis des Data Acts erheblich Druck aufeinander aufbauen. Dieser Aufsatz beleuchtet daher die wichtigsten Anspruchskonstellationen, die erforderlichen vertraglichen Regelungen zwischen den Akteuren und gibt praktische Hilfestellungen für Unternehmen.

1. Ansprüche aus dem Data Act für den Nutzer und Dritte

Die Regelungen in den Art. 3 bis 7 DA sollen das Ziel des Data Acts umsetzen: Daten leicht zugänglich zu machen. Die Vorschriften stellen daher ein Zugangskonzept dar, ausgehend vom direkten Zugriff des Nutzers, hin zu der Bereitstellungspflicht des Dateninhabers.

Aus Art. 3 Abs. 1 DA erwächst die Pflicht des Dateninhabers, vernetzte Produkte so zu konzipieren und herzustellen bzw. verbundene Dienste so zu konzipieren und zu erbringen, dass die Daten für den Nutzer einfach, sicher, unentgeltlich in einem umfassenden, strukturierten, gängigen und maschinen-lesbaren Format und direkt zugänglich sind. Der Dateninhaber muss dem Nutzer die Daten allerdings nur dann direkt zugänglich machen, soweit dies relevant und technisch durchführbar ist.

Wenn der Nutzer technisch nicht direkt vom vernetzten Produkt oder vom verbundenen Dienst auf die Produktdaten zugreifen kann, hat er einen Datenzugangsanspruch gegen den Dateninhaber nach Art. 4 Abs. 1 DA auf die ohne Weiteres verfügbaren Daten. Hierunter versteht Art. 2 Nr. 17 DA Daten, die ein Dateninhaber ohne unverhältnismäßigen Aufwand rechtmäßig von dem vernetzten Produkt oder verbundenen Dienst erhält oder erhalten kann. Voraussetzung für den Datenzugangsanspruch ist folglich, dass keine Zugangsmöglichkeit nach Art. 3 Abs. 1 DA besteht. Ausgelöst wird der Datenzugangsanspruch durch einfaches Verlangen des Nutzers.

Vorrangig werden dritte Wirtschaftsakteure ein Interesse an der Nutzung von Daten haben. Vor diesem Hintergrund muss der Dateninhaber nach Art. 5 Abs. 1 DA auf Verlangen eines Nutzers einem Dritten ohne Weiteres verfügbare Daten bereitstellen. Gatekeeper im Sinne des Digital Markets Acts sind jedoch vom Datenzugangsanspruch ausgeschlossen.

Art. 4 und 5 DA führen folglich dazu, dass jeder Nutzer eines vernetzten Produkts und nahezu jeder Dritte, der die Erlaubnis des Nutzers hat, Zugang zu den Daten erhalten muss, die das vernetzte Produkt oder der verbundene Dienst erzeugt.

2. Erforderliche Vertragsbeziehungen

Das bedeutet zugleich, dass sich Dateninhaber wie -nachfrager rechtzeitig um die entsprechende Vertragsgestaltung kümmern müssen. Unter dem Data Act werden drei Arten von Vertragsbeziehungen relevant:

1. Dateninhaber – Nutzer

Auch der Dateninhaber selbst darf nicht-personenbezogene Daten, die durch das Produkt oder den Dienst generiert werden, für eigene Zwecke künftig nur noch auf Grundlage eines Vertrages mit dem Nutzer, also mit dessen Erlaubnis, verwenden (Art. 4 Abs. 13 DA). Diese Erlaubnis wird voraussichtlich schon aus Praktikabilitätsgründen im Rahmen des Kauf-, Miet- oder Leasingvertrages über das jeweilige Produkt bzw. des Vertrages über die Erbringung des Dienstes eingeholt. Ein Kopplungsverbot, das den Dateninhaber daran hindern würde, die Nutzung eines Produkts oder Dienstes vom Abschluss entsprechender Vertragsklauseln abhängig zu machen, enthält der Data Act nicht (s. auch Erwägungsgrund 25).

Dem Nutzer sind vor Vertragsabschluss bestimmte Mindestinformationen bereitzustellen, so etwa die Art der Daten, die das vernetzte Produkt oder der Dienst generieren kann, sowie die Möglichkeiten für den Nutzer, darauf zuzugreifen (Art. 3 Abs. 3 und Abs. 4 DA). Dateninhaber dürfen zudem ihrerseits die generierten Produktdaten (Dienstdaten sind hier nicht genannt) Dritten nur zum Zweck der Erfüllung ihres Vertrages mit dem Nutzer bereitstellen (Art. 4 Abs. 14 DA). Ob hiervon wiederum vertraglich abgewichen werden kann, ist noch umstritten.

2. Dateninhaber – Dritter

Verlangt der Nutzer, dass der Dateninhaber einem Dritten Zugang zu den generierten Daten gewährt, erfordert das einen Vertrag zwischen dem Dateninhaber und dem benannten Dritten (Art. 8 DA). Der Dateninhaber muss dem Dritten die Daten zu fairen, angemessenen und nichtdiskriminierenden Bedingungen bereitstellen (Art. 8 Abs. 1 DA). Diese „FRAND“ Anforderung (Fair, Reasonable and Non Discriminatory) ist auch aus dem Patentrecht bekannt. Ähnlich wie dort dürfte es auch im Geltungsbereich des Data Act in der Praxis Schwierigkeiten der Bewertung von Bedingungen als „FRAND“ geben.

So darf der Dateninhaber für die Bereitstellung der Daten an Dritte eine Vergütung verlangen (für die Bereitstellung an den Nutzer dagegen nicht). Diese Vergütung soll die Kosten für die Bereitstellung der Daten und Investitionen in deren Erhebung berücksichtigen, ist aber – außer, der Datenempfänger ist ein KMU oder eine gemeinnützige Forschungseinrichtung – nicht auf diese Kosten beschränkt (Art. 9 Abs. 2 und 3 DA). Der Dateninhaber darf vielmehr eine Marge verlangen (Art. 9 Abs. 1 DA). Wie hoch diese Marge sein darf, ist allerdings offen. Laut Data Act soll die Kommission noch Leitlinien für die Berechnung der angemessenen Gegenleistung erlassen (Art. 9 Abs. 5 DA).

Die Vorgabe fairer Vertragsbedingungen zwischen Dateninhaber und Drittem wird flankiert durch einen Negativkatalog missbräuchlicher Vertragsklauseln (ähnlich der aus dem deutschen Recht bekannten AGB-Kontrolle). Die aufgeführten Vertragsklauseln, etwa Haftungsausschlüsse oder Kündigungshindernisse, sind unwirksam, wenn ein Unternehmen sie einem anderen einseitig auferlegt (Art. 13 DA).

3. Nutzer – Dritter

Zusätzlich schließt der Nutzer eine Vereinbarung mit dem Dritten ab, der auf Verlangen des Nutzers Daten von dem Dateninhaber erhalten soll. Der Dritte darf die so erhaltenen Daten nur so nutzen, wie mit dem Nutzer vereinbart. Insbesondere darf er sie nicht für andere als die vertraglich vereinbarten Zwecke einsetzen (Art. 6 Abs. 1 DA). Der Data Act räumt dem Nutzer insoweit die Kontrolle darüber ein, wie seine Daten (weiter) verwendet werden.

3. Handlungsempfehlungen

Unternehmen sollten zunächst analysieren, welche ihrer vernetzten Produkte und verbundenen Dienste in den Anwendungsbereich des DA fallen. Sodann sollten Unternehmen den Umfang der Daten identifizieren, die sie Nutzern bzw. Dritten zugänglich machen müssen: Hat der Nutzer nach Art. 3 Abs. 1 DA einen direkten Zugangsanspruch, erfasst dieser Produktdaten bzw. verbundene Dienstdaten. Der Datenzugangsanspruch nach Art. 4 Abs. 1 DA (bzw. Art. 5 Abs. 1 DA im Fall des Dritten), ist auf „ohne weiteres verfügbare Daten“ beschränkt (siehe dazu Ziff. 1).

Haben Unternehmen ein Interesse daran, Nutzern Daten nicht herauszugeben, sind die Möglichkeiten zur Begrenzung des Datenzugangsanspruchs zu prüfen: Dateninhaber können den Datenzugangsanspruch des Nutzers beispielsweise bei Fehlen einer hinreichenden datenschutzrechtlichen Rechtsgrundlage oder in eng begrenzten Fällen bei Vorliegen von Geschäftsgeheimnissen begrenzen bzw. ausschließen. In jedem Fall bedarf es einer Einzelfallprüfung für jedes Produkt bzw. jeden Dienst.

Möchten Unternehmen ein Produkt oder Service anbieten, für das oder für den sie selbst auf den Datenzugang gegenüber Dateninhabern angewiesen sind, sollten sie sicherstellen, dass die Anspruchsvoraussetzungen aus Art. 5 DA vorliegen und die erforderlichen vertraglichen Vereinbarungen mit dem Nutzer und Dateninhaber vorliegen, bevor sie das Produkt bzw. den Service auf den Markt bringen.

3. Data Act und DSGVO

(Wie) geht das zusammen?

Seit dem 12. September 2025 kommt ein Großteil der Verpflichtungen aus dem Data Act (Datenverordnung – DVO) zur Anwendung und damit sind u.a. für Anbieter vernetzter Produkte und verbundener Dienste in der Pflicht, bestimmten Akteuren Zugang zu Daten über die Nutzung zu gewähren. Hiervon sind prinzipiell personenbezogene und nicht personenbezogene Daten gleichermaßen betroffen, denn der Data Act findet auf beide Datenarten Anwendung (Art. 1 Abs. 2 DVO). Damit ist aber leider nicht automatisch gewährleistet, dass man sich künftig für Zwecke des Data Act eine differenzierte Betrachtung sparen könnte. Denn der Data Act trifft an vielen Stellen eben doch unterschiedliche Regelungen, je nachdem, ob es um personenbezogene Daten geht oder nicht:

- Kap. VII DVO gilt generell nur für nicht-personenbezogene Daten;
- Art. 4 (12) und 5 (7) DVO schränken die Herausgabepflicht des Dateninhabers nur bzgl. personenbezogener Daten ein;
- Der Vertragsvorbehalt und die Nutzungsbeschränkungen für Dateninhaber in Art. 4 (13) und (14) DVO gelten nur für nicht-personenbezogene Daten;
- Art. 5 (1) DVO enthält eine Sondervorschrift bzgl. personenbezogener Daten in dem Sinne, dass das darin verankerte Datenweitergaberecht die Rechte betroffener Personen nach DSGVO nicht beeinträchtigen darf.

Es bleibt somit dabei, dass die DSGVO Sonderregelungen für den Umgang mit personenbezogenen Daten trifft, die potenziell auch im Rahmen des Data Act beachtet werden müssen. Es ist also weiterhin notwendig, mit der Differenzierung zwischen personenbezogenen und nicht-personenbezogenen Daten umzugehen.

Auflösung von Differenzierungen durch pauschale Vorrangregelung?

Leider hilft es hierbei auch nicht weiter, pauschal von einem Vorrang der DSGVO vor der DVO auszugehen und auf diese Weise unliebsame Pflichten auf Datenzugangsgewährung nach der DVO pauschal auszuhebeln. Zwar statuiert Art. 1 Abs. 5 S. 1 DVO, dass der Data Act „unbeschadet“ der DSGVO gelte. Und nach ErwG 7 S. 2 DVO sei es so, dass die DVO das Unionsrecht zum Schutz personenbezogener Daten ergänzt und es unberührt lasse. Hierzu hat die Kommission in Ihrem am 3. Februar 2025 aktualisierten FAQ-Dokument zum Data Act sogar klargestellt: „The GDPR is fully applicable to all personal data processing activities under the Data Act. The Data Act does not regulate as such the protection of personal data.“

Diese Festlegungen sind aber leider unterkomplex und bestenfalls missverständlich. Sie bedeuten nach verständiger Auslegung der DVO gerade nicht, dass die DSGVO immer und pauschal der DVO vorginge. Das lässt sich an folgenden Regelungen ablesen:

- Nach Art. 1 Abs. 5 S. 3 DVO soll das Datenschutzrecht (nur) im Falle eines Widerspruchs zwischen DVO und DSGVO Vorrang besitzen;

- Der Data Act enthält Regelungen, die allgemein den Umgang mit „Daten“ regeln und somit gerade auch für personenbezogene Daten gelten sollen; z.B. Nutzungsbeschränkungen von Dritten nach Art. 6 DVO;

- Der Data Act enthält sogar vereinzelt Sonderregelungen auch gezielt nur zu personenbezogenen Daten; z.B. für den Fall der Einbeziehung von Auftragsverarbeitern bei der Datenzugangsgewährung (ErwG 29 DVO) oder bei Datenbereitstellungsverlangen nach Art. 17 (1) g) DVO.

Letztlich bestätigt auch die Kommission diese Auslegung, wenn sie in ihren FAQ ausführt: „In some cases, the Data Act specifies and complements the GDPR“.

Das bedeutet, dass Pflichten oder Verbote aus der DSGVO nicht pauschal etwaigen Pflichten nach der DVO entgegengehalten werden können. Es muss eine Prüfung im Einzelfall erfolgen, ob in concreto eine Pflichtenkollision besteht, die einen Regelungskonflikt mit sich bringt.

Wann liegt ein Regelungskonflikt vor?

Zu der Frage, wann ein solcher Regelungskonflikt besteht (der hier dann wirklich zu einer Unanwendbarkeit der DVO führen könnte) hat sich der EuGH bereits in einer durchaus vergleichbaren Fallgestaltung verhalten. Diese Rechtsprechung lässt sich hier als Auslegungsmaxime auch für die DVO heranziehen.

In seinem Urteil in Sachen Wind, hat der EuGH das Vorliegen eines Regelungskonflikts durch Auslegung von vergleichbaren Regelungen in Art. 3 der Richtlinie 2005/29 zu unlauteren Geschäftspraktiken und Art. 1 Abs. 4 der Universaldienstrichtlinie wie folgt bestimmt: (EuGH, Urt. v. 13.09.2018, Rs. C-54/17 und C-55/17, Tz. 60f.)

- Eine Kollision bedeutet eine Beziehung zwischen den Bestimmungen, die über eine bloße Abweichung oder einen einfachen Unterschied hinausgeht und eine Divergenz aufweist, die unmöglich durch Ausgleich überwunden werden kann.

- Eine Kollision liege demnach nicht vor, wenn die Regelungen das Nebeneinanderbestehen von zwei Sachverhalten ermöglichen, ohne sie verfälschen zu müssen.

- Eine Kollision besteht vielmehr nur dann, wenn ein Rechtsakt Verpflichtungen auferlegt, die mit denen aus anderem Rechtsakt unvereinbar sind.

Das bedeutet: Ein Regelungskonflikt mit der DSGVO, der zur Unanwendbarkeit einer DVO-Regelung führen könnte, bestünde hier praxisnah nur dann, wenn die DSGVO eine Datenverarbeitung verbietet, die die DVO aber zwingend verlangt. Kein Regelungskonflikt besteht hingegen, wenn z.B. die DVO eine Verarbeitung verlangt, die DSGVO aber eine solche nicht verlangt (wenn auch ermöglicht); in solchen Fällen ist eine Koexistenz beider Regelungsregime möglich, indem eben die DVO-Regelung mit Verpflichtungscharakter vorgeht.

Folgerungen für Datenzugangsszenarien

Was heißt das ganz konkret für praxisrelevante Fallgestaltungen im Zusammenhang mit Datenzugangsansprüchen nach Art. 4 ff. DVO:

- **Darf ein Unternehmen pauschal unter Verweis auf den Vorrang der DSGVO die Weitergabe personenbezogener Daten an einen Dritten verweigern? Nein:** Art. 5 Abs. 1 S. DVO verankert ein Recht des Nutzers, vom Dateninhaber die Weitergabe von Daten an Dritten zu verlangen. In Art. 5 Abs. 13 DVO ist eine eigenständige spezielle Regelung zur Beachtung der Rechte betroffener Personen gemäß DSGVO enthalten; diese ist hier zu beachten. Im Ergebnis bedarf es einer datenschutzrechtlichen Ermächtigungsgrundlage nach Art. 6 DSGVO; eine pauschale Verweigerung lässt sich aber nicht rechtfertigen.

- **Hebelt der Vorrang der DSGVO die strengere Löschpflicht aus dem Data Act bzgl. personenbezogener Daten aus, so dass Daten weiter und länger aufbewahrt werden dürfen? Nein:** Nach Art. 6 Abs. 1 S. 2 DVO muss der Dritte die erhaltenen (personenbezogenen) Daten löschen, sobald er sie für den vereinbarten Zweck nicht mehr benötigt. Diese spezielle Löschpflicht ist zwar strenger als Art. 17 DSGVO und sie enthält auch keine Ausnahme für personenbezogene Daten. Weil die DSGVO aber eben nur die Möglichkeit einer längeren Aufbewahrung schafft, jedoch keine Pflicht, ergibt sich kein über die Vorrangregelung aufzulösender Konflikt.

- **Kann ein Unternehmen unter Berufung auf die DSGVO Daten für andere Zwecke verarbeiten, auch wenn der Data Act dies verbietet? Nein:** Art. 6 Abs. 1 S. DVO verbietet es dem Dritten, die ihm bereitgestellten Daten zu anderen Zwecken zu nutzen als mit dem Nutzer vereinbart. Diese Zweckbindungsregelung ist strenger als diejenige in 6 Abs. 4 DSGVO. Dennoch ist es dem Dritten verwehrt, eine Zweckänderung entgegen der DVO-Regelung nun auf Basis der DSGVO vorzunehmen; denn auch hier ermöglicht die DSGVO eine solche Zweckänderung nur, verlangt sie aber nicht, so dass wiederum kein echter Konflikt besteht und der Data Act Vorrang genießt.

- **Darf ein Unternehmen die Herausgabe personenbezogener Daten an einen Dritten verweigern, wenn es hierfür keine Rechtsgrundlage nach der DSGVO besitzt? Ja:** Art. 5 Abs. 1 S. DVO verankert

zwar, wie schon dargelegt, ein Recht des Nutzers, vom Dateninhaber die Weitergabe von Daten an einen Dritten zu verlangen; für den Fall, dass sich die Daten nicht (nur) auf den Nutzer, sondern eine andere natürliche Person beziehen, benötigt der Dateninhaber nach Art. 5 Abs. 7 DVO hierfür aber eine datenschutzrechtliche Ermächtigungsgrundlage im Sinne von Art. 6 DSGVO. Weil sich diese Anforderung sogar direkt aus der DVO ergibt, stellt sich die Frage der Vorrangigkeit der DSGVO hier gar nicht.

Im Ergebnis zeigt sich, dass entgegen der landläufigen Vorstellung, die DSGVO genieße Vorrang vor dem Data Act, letzterer auch für den Umgang mit personenbezogenen Daten häufig verbindliche Vorgaben macht, die strenger sind als die DSGVO und ihr trotzdem vorgehen. Verarbeitungsrestriktionen nach der DVO sind somit zusätzlich zur DSGVO zu beachten. Unternehmen müssen dies durch eine entsprechende Anpassung auch ihrer Datenschutz-Governance berücksichtigen.

Notwendigkeit der Feststellung des Personenbezugs der Daten

Das bedeutet aber auch, dass die vom Data Act betroffenen Unternehmen nicht darauf verzichten können, die verarbeiteten Daten richtig zu qualifizieren – also als personenbezogen oder als nicht personenbezogen. Denn nur dann kann eine Einhaltung von DVO und DSGVO gewährleistet werden. Diese Feststellung bleibt diffizil. Bisher hatten sich manche Unternehmen deshalb bei der Frage, ob auf einen Datenbestand die DSGVO angewendet wird oder nicht, für einen vorsichtigen Ansatz entschieden und sind quasi vorsorglich von einem Personenbezug ausgegangen. Dieser Ansatz wird im Anwendungsbereich des Data Act nicht mehr möglich sein, denn er könnte dazu führen, dass bestimmte Daten (wegen ihres vermeintlichen Personenbezugs) ungerechtfertigt vom Datenzugang ausgenommen werden.

Im Ausgangspunkt kommt es den Rechtsanwendern hier zumindest entgegen, dass die Frage des Personenbezugs nach DVO und DSGVO einheitlich bewertet wird und es deshalb nicht zu definitorischen Unschärfen kommen kann: Nach Art. 2 Nr. 3 und 4 DVO sind „personenbezogene Daten“ im Sinne der DVO solche im Sinne des Art. 4 Nr. 1 DSGVO.

Den Erwägungsgründen der DVO ist ferner zu entnehmen, dass bei Datensätzen mit untrennbar verbundenen personenbezogenen und nicht-personenbezogenen Daten insgesamt von einem Personenbezug ausgegangen werden solle (ErwG 34 DVO).

Leider ist auch bisher unter der DSGVO im Detail höchst unklar, wie personenbezogene Daten genau von nicht-personenbezogenen – also anonymen – Daten abzugrenzen sind. Weil die Frage des Personenbezugs zudem relativ und nicht absolut zu bestimmen ist und deshalb von den Möglichkeiten und der Wahrscheinlichkeit einer Identifizierung der jeweiligen Stelle abhängt, verbieten sich pauschale Klassifizierungen ohnehin. Eine „echte“ Anonymisierung, also ein vollständiger Entfall des Personenbezugs sämtlicher Daten, bleibt schwierig zu realisieren. Für den Dateninhaber wird ein Datensatz ggf. schon anonym sein, wenn bestimmte Identifier gelöscht werden. Für den Nutzer aber, der als juristische Person bspw. Arbeitgeber mehrerer nutzender Personen eines vernetzten Geräts ist, ist eine Zuordnung aus dem Zusammenspiel von Nutzungsdaten eventuell dennoch möglich.

Rechtfertigung von nach DVO gebotenen Datenverarbeitungen

Ist festgestellt, dass bei einem Datenzugangsverlangen personenbezogene Daten zu verarbeiten sind, bedarf es einer Rechtfertigung nach Maßgabe der DSGVO. Der Data Act selbst rechtfertigt die Datenverarbeitung explizit nicht. Es kommen somit die Rechtsgrundlagen aus Art. 6 DSGVO zur Anwendung. Gerade wenn es um eine Weitergabe der Daten von betroffenen Personen, die keine Nutzer sind, an Dritte nach Art. 5 DVO geht, wird für den Dateninhaber zumeist nur eine Verfolgung berechtigter Interessen im Sinne von Art. 6 Abs. 1 lit. f DSGVO in Betracht kommen, weil weder ein Vertragsverhältnis noch ein direkter Kontakt mit der betroffenen Person besteht (sondern nur mit dem Nutzer). Ob diese Interessenabwägung dann aber regelmäßig zugunsten des Dateninhabers ausgehen wird, steht angesichts der äußerst strengen Rechtsprechung des EuGH zu diesem Rechtfertigungsgrund in den Sternen:

- In einer der Urteile in Sachen Meta Platforms hat der EuGH postuliert, dass die Erlaubnistatbestände in Art. 6 Abs. 1 lit. b bis lit. f DSGVO (mithin alle Erlaubnistatbestände außer der Einwilligung) generell eng aus[zu]legen seien, da sie dazu führen können, dass eine Verarbeitung personenbezogener Daten trotz fehlender Einwilligung der betroffenen Person rechtmäßig ist (EuGH, Urt. v. 4.7.2023 – C-252/21, Rn. 93).

- Nach der Entscheidung des EuGH in Sachen Mousse soll zudem das objektive Vorliegen eines berechtigten Interesses allein nicht ausreichend sein, sondern es müsse den betroffenen Personen das verfolgte berechtigte Interesse zum Zeitpunkt der Erhebung der Daten auch unmittelbar mitgeteilt worden sein, damit eine Datenverarbeitung auf Art. 6 Abs. 1 lit. f DSGVO gestützt werden könne (EuGH, Urt. v. 9.1.2025, C-394/23, Rn. 52).

- In der Entscheidung Koninklijke Nederlandse Lawn Tennisbond versteigen sich die Luxemburger Richter gar zu der These, dass der Verantwortliche zudem allen anderen ihm obliegenden Pflichten aus der DSGVO nachkommen müsse, damit die Wahrnehmung eines

berechtigten Interesses eine Verarbeitung personenbezogener Daten gemäß Art. 6 Abs. 1 lit. f DSGVO rechtfertigen könne (EuGH, Urt. v. 4.10.2024, C-621/22, Rn. 50).

Während Unternehmen bei der Rechtfertigung eigennütziger Verarbeitung über die Interessenabwägung regelmäßig einen großzügigen Maßstab anlegen, werden die Dateninhaber hier vermutlich sehr viel vorsichtiger agieren und im Zweifel einer strengen Auslegung der DSGVO das Wort reden, um keinen Datenschutzverstoß zu begehen.

Sonstige Wechselwirkungen zwischen DVO und DSGVO

Aber auch jenseits des Aspekts der Zulässigkeit, Daten mit oder ohne Personenbezug für Zwecke des Data Act zu verarbeiten, bestehen Wechselwirkungen zwischen DVO und DSGVO, die Unternehmen zu beachten haben. Ein praxisrelevantes Beispiel stellt die Betroffenheit von Auftragsverarbeitern dar. Kommen Auftragsverarbeiter auch im Anwendungsbereich des Data Act zum Einsatz, sind besondere Vorkehrungen zu treffen:

- Auftragsverarbeiter sind zwar selbst nicht als Dateninhaber zu qualifizieren (ErwG 22 S. 4 DVO), nach ErwG 29 S. 2 DVO sollen Dateninhaber aber sicherstellen, dass Zugangsverlangen auch von etwa eingeschalteten Auftragsverarbeitern entgegengenommen und bearbeitet werden. Es empfiehlt sich deshalb, die Auftragsverarbeitungsverträge um entsprechende Weisungsbefugnisse zu ergänzen;

- Zudem ist es so, dass die Verneinung der Eigenschaft als Dateninhaber nur gilt, soweit die Daten auch im Auftrag verarbeitet werden. Zunehmend tauchen aber Mischformen der Zusammenarbeit auf, in denen Auftragsverarbeiter bestimmte Verarbeitungen außerhalb der Weisungsbindung für eigene Zwecke verarbeiten; z.B. zum Zwecke des Trainings von KI-Modellen. Insoweit fungiert der Auftragsverarbeiter dann aber als eigenständiger Verantwortlicher und unterliegt seinerseits einer Herausgabepflicht als Dateninhaber unter dem Data Act.

Fazit und Empfehlungen

Das Zusammenspiel von Data Act und DSGVO ist hochkomplex. Anstatt einer vermeintlich einfachen und pauschalen Vorrangregelung zugunsten der DSGVO gibt eine Vielzahl von Verschränkungen und Verflechtungen, deren Tauglichkeit sich erst in der Praxis erweisen muss. Egal ob als potenzieller Anspruchsteller oder Anspruchsverpflichteter nach dem Data Act sollten Unternehmen die möglichen Auswirkungen bereits vor der Konfrontation mit konkreten Daten-Herausgabeverlangen genau untersuchen, um im Vorfeld die Weichen für eine datenschutzkonforme Umsetzung des Data Act zu stellen. Folgende Maßnahmen seien beispielhaft benannt:

- Prüfung und Update der Datenklassifizierungen, um der veränderten Bedeutung nicht-personenbezogener Daten nach dem Data Act Rechnung zu tragen;

- Prüfung und ggf. Anpassung des Verantwortlichkeitskonzepts, um festzustellen, wer für welche Verarbeitung als datenschutzrechtlich „Verantwortlicher“ als Dateninhaber nach dem Data Act zu qualifizieren ist;

- Prüfung und ggf. Anpassung des Datennutzungskonzepts (einschließlich des Sperr- und Löschkonzepts und des Zugriffskonzepts) angesichts der über die DSGVO-Vorgaben hinausgehenden Anforderungen an Zweckbindung, Löschung etc.;

- Ergänzung der Datenschutzerklärungen um diejenigen berechtigten Interessen, auf die ggf. Datenweitergaben und andere -verarbeitungen nach dem Data Act gestützt werden;

- Anpassung von Einwilligungen und Nutzungsverträgen zur Verankerung rechtfertigungsbedürftiger, vom Data Act ausgelöster Datenverarbeitungen;

- Prüfung und Ergänzung sowohl von Auftragsverarbeitungsverträgen als auch von Verträgen über gemeinsame Verantwortlichkeit, um angemessene Weisungen bzw. Vereinbarungen zur Ermöglichung von Datenzugangsgewährungen zu integrieren.

4. Der Data Act reguliert das Cloud Switching – und beeinflusst das Verhältnis von Kunden und Cloud-Anbietern

Neben Regelungen zu Zugang und Nutzung von Daten enthält der Data Act – etwas versteckt – auch komplexe Regelungen zum Wechsel von Cloud-Providern, die ebenso massive Auswirkungen für Provider wie für Kunden von Cloud-Diensten haben können.

Als Teil der europäischen Datenstrategie zielt der Data Act auf das Aufbrechen sog. Datensilos, die Verbesserung der Interoperabilität von Software und allgemein der Datennutzung. Die neuen Regeln sollen es ermöglichen, das Potential datengesteuerter Geschäftsmodelle voll auszuschöpfen, um so Innovation innerhalb der EU zu fördern. Seit dem 12. September 2025 findet der Data Act unmittelbare Anwendung innerhalb der EU.

Kapitel VI des Data Acts (Art. 23 bis 31) sieht zwingende Regelungen für Vertragsverhältnisse zwischen sog. Datenverarbeitungsdiensten (also vor allem Anbieter von Cloud-Diensten) und deren Kunden vor. Hierdurch soll u.a. der Wechsel zwischen Datenverarbeitungsdiensten erleichtert werden, wodurch so ein sog. „Vendor Lock-In“ von Kunden verhindert werden soll. Im Folgenden stellen wir vor, welcher Anpassungsbedarf diese Regelungen konkret für Cloud-Anbieter zur Folge haben und wie diese (zumindest nach Ansicht des Gesetzgebers) den Kunden von Cloud-Diensten dadurch helfen. Die Europäische Kommission hat zudem einen ersten Entwurf von Standardvertragsklauseln nach Art. 41 Data Act veröffentlicht, welche einen Schluss darauf zulassen, wie sich die Kommission die Umsetzung des Kapitels VI vorstellt.

Worum geht es beim Cloud Switching?

Der Data Act verpflichtet Anbieter von Cloud-Diensten dazu, diese so anzubieten, dass ein Wechsel der Kunden zu einem anderen Cloud-Anbieter oder ein Wechsel zu einer sog. „On-Premise“-Lösung jederzeit und unproblematisch möglich ist. Dies soll durch zahlreiche Regelungen, die die vertragliche Ausgestaltung von Cloud-Verträgen betreffen, erreicht werden. So sollen z.B. eine zweimonatige Kündigungs- und dreißig Tage Wechselfrist vertraglich verankert werden. Die Möglichkeit, für die Unterstützung beim Wechsel zu einem neuen Anbieter ein Wechselentgelt zu verlangen, wird stark eingeschränkt und es werden weitreichende Beendigungs- und Unterstützungspflichten vorgeschrieben. Die Art. 30 ff. Data Act enthalten zudem technische Vorgaben an die Interoperabilität und verpflichten bspw. zum Bereitstellen von Schnittstellen für Wechsel-Tools.

Zentrale Pflichten

Art. 23 Data Act ist die zentrale Norm und Ausgangspunkt für die Verpflichtungen von Anbietern von sog. Datenverarbeitungsdiensten. Diese müssen umfangreiche Maßnahmen ergreifen, um Hindernisse bei einem Wechsel

des Kunden zu einem anderen Anbieter oder auch in eine unternehmensinterne IT-Infrastruktur („On-Premise“) zu beseitigen. Gleichzeitig soll auch die Nutzung mehrerer Datenverarbeitungsdienste im Parallelbetrieb über eine einheitliche Nutzeroberfläche gewährleistet werden (die sogenannte Interoperabilität von Datenverarbeitungsdiensten, siehe Art. 23 i. V. m. Art. 31 Data Act).

Art. 23 schafft Mindestverpflichtungen für Datenverarbeitungsdienste und schreibt vor, sämtliche kommerzielle, gewerbliche, technische, vertragliche und organisatorische Hindernisse auszuräumen, die den Vollzug des Wechsels zwischen Cloud-Anbietern verhindern. Hier hatte der Gesetzgeber die vereinzelt hohen Wechselkosten und technisch-faktischen Wechselhindernisse auf Anbieterseite im Blick, die Nutzer von Cloud-Diensten daran hindern könnten, einen (kommerziell grundsätzlich sinnvollen) Wechsel tatsächlich vorzunehmen.

Datenverarbeitungsdienste als Adressaten

Der Data Act verpflichtet sog. „Datenverarbeitungsdienste“. Dabei handelt es sich laut der Definition aus Art. 2 Nr. 8 Data Act um Anbieter einer „digitalen Dienstleistung, 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“.

Nach Erwägungsgrund 81 können darunter Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) und Infrastructure-as-a-Service (IaaS) fallen.

Anbieter von Datenverarbeitungsdiensten im Sinne des Data Acts sind sowohl der ursprüngliche Anbieter, mit dem ein Kunde ein bestehendes Vertragsverhältnis hat, als auch der übernehmende Anbieter, zu dem ein Kunde wechseln möchte. Wie die einzelnen Merkmale genau auszulegen sind, ist leider noch ziemlich offen. Das Zurverfügungstellen von einzelnen, klar definierten Hardware-Ressourcen, die nur ein Kunde benutzt, fällt jedenfalls nicht darunter. Sobald eine gewisse Flexibilität in das Angebot eines Datenbank- bzw. Storage Space-Anbieters kommt, ist jedoch jeder Dienst einzeln darauf zu untersuchen, ob ein Datenverarbeitungsdienst vorliegt.

Bereichsausnahmen für Individuallösungen

Art. 31 Data Act macht Bereichsausnahmen von den hier genannten Pflichten. So sind etwa Verarbeitungsdienste, bei denen die meisten zentralen Funktionen kundenspezifisch zugeschnitten wurden (Art. 31 Abs. 1 Alt. 1 Data Act), Individualsoftware (Art. 31 Abs. 1 Alt. 2 Data Act) sowie zeitweise für Test- oder Bewertungszwecke überlassene Software (Art. 31 Abs. 2 Data Act) vom Anwendungsbereich ausgeschlossen. Die Vorschriften der Art. 23 ff. Data Act finden aufgrund der Bereichsausnahmen grundsätzlich nur Anwendung auf sog. „One-To-Many“-Lösungen, deren genaue Definition und Abgrenzung jedoch im Einzelnen schwierig sein kann.

Denkbar ist etwa der Fall, dass eine SaaS-Lösung gegebenenfalls durch eine kundenspezifische Implementierung Software aus dem Anwendungsbereich fallen könnte. In der Praxis könnte sich hieraus die folgende Schwierigkeit ergeben: Der Anbieter muss den Nutzer nämlich bereits vor Vertragsschluss über eine derartige bestehende Bereichsausnahme informieren (siehe Art. 31 Abs. 3 Data Act). Wenn der Scope der vorzunehmenden Implementierung aber – wie dies typischerweise der Fall ist – vor Vertragsschluss noch gar nicht feststeht, ist eine rechtssichere Aussage hierzu kaum möglich.

Die Wechselvorschriften des Art. 23 Data Act finden zudem nur dann Anwendung, wenn die „gleiche Dienstart“ bei Erst- und Ziel – bzw. Wechselanbieter vorliegt. Dies bedeutet gemäß der Definition in Art. 2 Nr. 9 Data Act, dass der Datenverarbeitungsdienst „dasselbe Hauptziel“, „dieselben Hauptfunktionen“ sowie dasselbe Dienstmodell für die Datenverarbeitung kumulativ aufweisen muss (vgl. auch Erwägungsgrund 81 Data Act).

Weitere Pflichten nach Art. 23 ff. Data Act

Die in Art. 23 ff. Data Act genannten Pflichten gelten auch, wenn der Nutzer nur einen bestimmten Dienst aus einem größeren Vertrag herauslöst und zu einem anderen Anbieter verlegen möchte.

Anbieter von IaaS-Datenverarbeitungsdiensten (gemeint ist der ursprüngliche Anbieter) sind zudem verpflichtet, „alle ihm vernünftigerweise zur Verfügung stehenden Maßnahmen“ zu ergreifen, um zu ermöglichen, dass nach dem Wechsel des Kunden zu einem neuen Diensteanbieter der gleichen Dienstart bei der Nutzung durch den Kunden Funktionsäquivalenz erreicht wird (vgl. auch Erwägungs-grund 92 Data Act). Nach Art. 30 Abs. 1 Data Act bedeutet dies konkret, dass der ursprüngliche Anbieter angemes-sene Informationen, die technische Dokumentation, aber auch technische Unterstützung sowie Kapazitäten und gegebenenfalls die erforderlichen Instrumente zur Verfü-gung stellen muss.

Sonstige Anbieter von PaaS oder SaaS müssen zukünftig sowohl ihren Kunden als auch den neuen Anbietern, zu denen ein Kunde wechseln möchte, unentgeltlich eine offene Schnittstelle auf die betriebenen Dienste zur Verfügung stellen. Diese Schnittstelle wird gefordert, „um den Wechsel zu ermöglichen” (vgl. Art. 30 Abs. 2 Data Act). Um dem Kunden und dem neuen Anbieter die Implementierung der Schnittstelle zu ermöglichen, muss der bisherige PaaS-/SaaS-Anbieter zudem die hierfür notwendige Dokumentation bereitstellen.

Für sämtliche erfasste Dienstanbieter wird sich noch zeigen müssen, ob in Ausnahmefällen auch ein Tätigwerden auch noch nach dem vollzogenen Anbieterwechsel geschuldet ist. Der Gesetzestext schließt dies zumindest nicht aus, stellt jedoch auch keine Pflicht auf, den Erfolg der Funktionsäquivalenz herbeizuführen, sondern sieht

lediglich die „Ermöglichung“ geschuldet. Jedenfalls wäre ein solches Tätigwerden nach vollzogenem Wechsel nicht mehr von den schrittweise auf null zu reduzierenden Wechselentgelten erfasst, sodass hierfür wohl auch in Zukunft Gebühren erhoben werden dürften.

Diese Pflichten haben jedoch auch Grenzen: Anbieter von Datenverarbeitungsdiensten sind nicht verpflichtet, ihr geistiges Eigentum oder Geschäftsgeheimnisse gegenüber einem Kunden oder einem anderen Anbieter offenzulegen oder gar neue Technologien oder Dienste zu entwickeln.

Art. 25 Data Act: konkrete vertragliche Regelungen sind nun verpflichtend aufzunehmen

Art. 25 Data Act regelt, welche konkreten Regelungen ein Vertrag als Mindestinhalt enthalten muss und konkretisiert damit die in Art. 23 Data Act genannten Pflichten (s.o.). Zunächst müssen die Rechte und Pflichten des Kunden sowie die Pflichten des Anbieters in Bezug auf den Anbieterwechsel in einem schriftlichen Vertrag festgehalten werden (Art. 25 Abs. 1 Satz 1 Data Act).

Wechselrecht und Kontinuität des Geschäftsbetriebs

Der Vertrag muss Klauseln enthalten, nach denen der Kunde die Möglichkeit hat, zu einem anderen Datenverarbeitungsdienst zu wechseln (Art. 25 Abs. 2 lit. a Data Act). Neben der Möglichkeit des Wechsels hat der Datenverarbeitungsanbieter dafür Sorge zu tragen, dass der Geschäftsbetrieb bei einem Wechsel aufrechtgehalten wird (Art. 25 Abs. 2 lit. a ii) Data Act), d. h. das Wechsel- und Datenextraktionsbegehren des Kunden muss erfüllt werden und darf nicht zu Unterbrechungen führen. Sollte es doch zu Unterbrechungen kommen, bestehen insoweit Unterrichtungspflichten (Art. 25 Abs. 2 lit. a (iii) Data Act).

Kündigungsfrist

Ausdrücklich legt Art. 25 Abs. 2 lit. d Data Act auch eine Kündigungsfrist des Nutzers von maximal zwei (2) Monaten für einen solchen Anbieterwechsel fest. Diese Kündigungsfrist bzw. Vorlauffrist beginnt, indem der Nutzer den Anbieter über sein Wechselbegehren informiert. Während bei Clouddiensten die ordentliche Kündigungsfrist in vielen Fällen ausgeschlossen ist, ist dies eine erhebliche Stärkung der Rechte von Kunden.

Gebühren und Übergangsfrist

Zu beachten ist jedoch, dass weiter die Möglichkeit besteht, Stornierungsgebühren oder Vertragsstrafen bei einer vorzeitigen Kündigung des Vertrages zu vereinbaren, Art. 29 Abs. 4 Data Act, Erwägungsgrund 89 Data Act. Diese müssen im Einklang mit nationalem und EU-Recht stehen, verhältnismäßig (vgl. Erwägungsgrund 89) und gem. Art. 23 Data Act kein „kommerzielles Wechselhindernis“ darstellen. Anbieter stehen hier also vor der schwierigen Aufgabe, angemessene Modelle, die sie gegen das nun aufkommende Risiko einer jederzeit mit zwei Monaten Vorlauf erklärbaren Kündigung des Kunden absichern und gleichzeitig nicht unangemessen hohe Strafen zu vereinbaren. Hier gibt die Entwurfsversion der SCCs nur begrenzte Orientierungshilfe. Hintergrund dessen ist, dass die tatsächlichen Wechselumstände verschiedentlicher Natur sein können und die SCC daher lediglich allgemeingehaltene Verpflichtungen enthalten.

In dem jeweiligen Vertrag muss darüber hinaus auch eine verbindliche Übergangsfrist von maximal dreißig (30) Tagen vorgesehen sein, Art. 25 Abs. 2 lit. a Data Act. Ist die Einhaltung der Übergangsfrist dem Anbieter aus technischen Gründen nicht möglich, ist im Einzelfall eine Verlängerung des Übergangszeitraums auf maximal sieben (7) Monate bei Vorliegen der Voraussetzungen in Art. 25 Abs. 4 Data Act möglich.

Verlängerung und Übergangszeitraum

Dem Kunden muss zudem die Möglichkeit gegeben werden, den Übergangszeitraum einmal für die Dauer zu verlängern, die er für seine Zwecke angemessen hält, Art. 25, Abs. 5 Data Act. Der Vertrag gilt gemäß Art. 25 Abs. 2 lit. c Data Act nach einem erfolgreichen Vollzug des Wechsels als beendet. Die Daten müssen nach Art. 25 Abs. 2 lit. g Data Act für mindestens dreißig (30) Tage – gerechnet ab Beendigung des Übergangszeitraums – weiter abrufbar sein. Darüber hinaus muss der Anbieter eine Garantie dafür übernehmen, dass er nach dem erfolgreich vollzogenen Wechsel die exportierbaren Daten und digitalen Vermögenswerte des Kunden löscht (Art. 25 Abs. 2 lit. h Data Act).

Weiter sind nach Art. 27 Data Act alle Beteiligten verpflichtet, nach den Grundsätzen von Treu und Glauben zu handeln. Darunter fällt z. B., dass die Beteiligten die Daten sicher und fristgemäß übertragen und ein gängiges maschinenlesbares Format verwenden, vgl. Erwägungsgrund 97 Data Act.

Art. 26 Data Act sieht weitere Informationspflichten für Anbieter von Datenverarbeitungsdiensten hinsichtlich der Umsetzung des Wechsels vor und Art. 30 Data Act enthält Pflichten für die technische Umsetzung des Wechsels.

Schließlich sollen Wechselentgelte, d. h. Entgelte, die Anbieter für die Durchführung eines Wechsels erheben, schrittweise bis 2027 abgeschafft werden. Somit tragen in Zukunft die Anbieter von Cloud-Diensten das finanzielle Risiko aufwendiger und technisch komplexer Wechselvorhaben Diese sollten daher bereits bei der Entwicklung von Cloud-Produkten (noch mehr als bereits Praxis) beachtet werden. Zwar können Zusatzdienste, die über die im Data Act vorgeschriebenen Wechselunterstützung kostenpflichtig erbracht werden. Hier ist jedoch ebenfalls darauf zu achten, dass kein kommerzielles Wechselhindernis im Sinne des Art. 23 Data Act entsteht.

Folgen eines Verstoßes gegen Art. 25 Data Act

Neben einer öffentlich-rechtlichen Durchsetzung durch die Behörden ist auch eine zivilrechtliche Durchsetzung durch die Kunden oder Mitbewerber etwa über das Wettbewerbsrecht oder über die Wirksamkeitskontrolle des

AGB-Rechts zu erwarten. Der Verweis auf das Bußgeldregime der DSGVO erfasst explizit nicht die Regeln des Kapitels VI, die dieser Beitrag behandelt. Es bleibt daher abzuwarten, wie die nationalen Gesetzgeber und Aufsichtsbehörden hier vorgehen.

Bei Unwirksamkeit einzelner Klauseln, weil sie gegen den Data Act verstoßen, ist auf das geltende (AGB-)Recht zurückzugreifen. Bei Cloud-Verträgen mit Verbrauchern ist insbesondere zu beachten, dass sich die Pflichten aus dem Data Act mit den Pflichten für Cloud-Anbieter aus der Digitalvertragsrichtlinie (2019/770) sowie der Warenkaufrichtline (2019/771), beide im BGB umgesetzt, überschneiden können.

Entwurf der Standardvertragsklauseln (SCCs)

Im Hinblick auf Switching-Anforderungen (Kapitel VI DA) wird die EU-Kommission verschiedene Sets an SCCs veröffentlichen, die sich weitgehend untereinander ergänzen sollen, aber auch separat verwendet werden können.

Die SCCs werden im Gegensatz zu den aus dem Datenschutzrecht bekannten SCCs unverbindlich sein. Die Parteien können diese also nutzen und entsprechend ihren vertraglichen Bedürfnissen explizit an die eigenen Dienste und Wünsche bzgl. des Wechselszenarios anpassen. Das ist zunächst zu begrüßen, da so der Anpassungsbedarf in den Fachabteilungen und Prozessen an ein starres Set an Regeln wegfällt und die Data Act Compliance hier flexibler gestaltet werden kann.

Bei der Überarbeitung der SCCs ist jedoch der folgende Punkt zu beachten: Die SCCs sind so entworfen, dass sie im Einklang mit den im Data Act vorgesehenen Rechten und Pflichten formuliert sind und auch untereinander kohärent sein sollen. Daher sollten die jeweiligen Parteien die SCC-Texte kritisch prüfen, inwieweit diese auf den konkreten Einzelfall hin überhaupt angepasst werden können und gleichzeitig die Pflichten nach dem Data Act ausreichend abbilden.

Die bereitgestellten SCCs dienen als Muster für aus Sicht der Kommission bewährte Verfahren, mit denen die Verpflichtungen vertraglich umgesetzt werden können. Die Klauseln sind relativ eindeutig formuliert und regeln, was wann geschieht und wen die entsprechenden vertraglichen Verpflichtungen treffen.

Zum Stand April 2025 waren folgende Themen für die Standardvertragsklauseln in Bearbeitung: General; Termination; Switching & Exit; Security and Business Continuity; Liability; Non-Dispersion; Non-Amendment.

Die SCCs sind ein hochkomplexes Werk von Vertragsklauseln, das für Klauseln für mehrere Szenarien enthält (etwa den Einsatz von Self-Service Wechsel Tools). Was sich jedoch klar herauskristallisiert: Neben der teilweise im Wortlaut mit den Pflichten des Data Act identischen Klauseln, enthalten die SCCs ausführliche Exit-Pläne, die Platzhalter für alle zu machenden Angaben enthalten.

Aktuelle Handhabung der großen Anbieter

Viele Anforderungen des Data Act gehen weit über die gängige Praxis hinaus. Kunden könnten hier gegebenenfalls prüfen, inwiefern sie in Zukunft flexibler sind. Auch erwarten wir eine Veränderung der Verhandlungspositionen in Beschaffungsverfahren und den damit einhergehenden Vertragsverhandlungen. Cloud-Anbieter sollten ihre AGB bis zum Geltungsbeginn des Data Acts unbedingt überarbeitet haben und sorgfältig prüfen, wo sie tatsächlich in den Anwendungsbereich fallen und wie sie mit den Stellen umgehen, an denen der Data Act unklar formuliert ist und Spielraum bietet.

Daneben birgt für die Cloud-Anbieter auch die technische Umsetzung der Vorgaben aus Art. 25 Abs. 2 Data Act bis zum Geltungsbeginn im September 2025 noch Herausforderungen. Beispielsweise bleibt unklar, wie die geforderte „angemessene Unterstützung“ für den Wechsel seitens der Datenverarbeitungsdienste nach Art. 25 Abs. 2 lit. a (i) Data Act technisch umzusetzen ist: Was ist „angemessen“? Welche technischen Leistungen müssen mindestens erbracht werden, damit der Wechsel „angemessen“ unterstützt wird?

Ausblick

Auch wenn aktuell sicherlich noch einige Fragezeichen hinsichtlich der in Art. 23 ff. Data Act festgelegten Pflichten bestehen, sind die Änderungen für die Nutzer und Anbieter von Cloud-Diensten erheblich. Die nun zwingend vorgeschriebene Interoperabilität und die gesetzlich verpflichtende Möglichkeit, einen Datenverarbeitungsdienst zu wechseln, wird die Verhandlungsmacht von Nutzerunternehmen gegenüber den großen Cloud-Anbietern steigern.

Anbieter von Cloud-Diensten werden durch die Umsetzung des Data Acts vor erhebliche Herausforderungen gestellt. Neben den organisatorischen und vertraglichen Anpassungen sind auch weitreichende technische Veränderungen der angebotenen Produkte vorzunehmen.

Konkrete Timeline

Der Data Act wurde am 13. Dezember 2023 verabschiedet und trat am 11. Januar 2024 in Kraft.

Die in diesem Beitrag behandelten Pflichten gelten für alle Verträge seit dem 12. September 2025 (Art. 50 S. 2 Data Act). Es findet eine stufenweise Abschaffung von Wechselentgelten für den Vollzug von Anbieterwechseln bis zum 12. Januar 2027 (Art. 29 Abs. 1, 2 Data Act) statt.

5. Datenbereitstellung an den Staat und die EU

Der Data Act beinhaltet geradezu ein „Sammelsurium“ aus Regelungen zum Umgang mit anonymen und personenbezogenen Daten. Wenn man eine gemeinsame Klammer der verschiedenen Kapitel finden mag, wäre dies die Erleichterung des Zugangs zu Daten innerhalb bestimmter – häufig auch vertraglich flankierter – Regeln.

Eine besondere Nuance im Data Act enthält dabei das Kapitel V („Bereitstellung von Daten für öffentliche Stellen, die Kommission, die Europäische Zentralbank und Einrichtungen der Union wegen außergewöhnlicher Notwendigkeit“). Wie der Titel schon sagt, geht es um Pflichten von Dateninhabern, öffentlichen Stellen der Mitgliedstaaten oder der EU in bestimmten außergewöhnlichen Situationen Daten bereitzustellen.

Beteiligte Parteien

Berechtigt sind dabei öffentliche Stellen der Mitgliedstaaten und der EU. Dies gilt sogar grenzüberschreitend. Beispielsweise könnte eine deutsche Behörde im Fall des Fischsterbens in der Oder von einem polnischen Unternehmen Daten zur Verwendung bestimmter Chemikalien verlangen. In diesem Fall käme es jedoch nicht zu einem direkten Datenherausgabeverlangen, sondern zu einem Vorgehen „über Eck“. Die für das jeweilige Unternehmen zuständige Aufsichtsbehörde, hier also die polnische Behörde, koordiniert sodann das Verfahren (Art. 22 Data Act).

Verpflichtet sind in erster Linie Unternehmen (nicht aber andere öffentliche Stellen), nach den Ausführungen in ErwGr 63 wohl auch öffentliche Unternehmen. Diese Unternehmen müssen „Dateninhaber“ nach dem Data Act („DA“) sein, also nach der – leider zirkulären – Definition aus Art. 2 Nr. 13 DA eine Person, die nach dem Data Act oder einem anderen Gesetz berechtigt oder verpflichtet ist, Daten zu nutzen und bereitzustellen, die sie während der Erbringung eines verbundenen Dienstes abgerufen oder generiert hat. Interessanterweise hat der Unionsgesetzgeber damit anscheinend im Grundsatz darauf verzichtet, beispielsweise Restaurants zur Herausgabe von Gästedaten zu verpflichten, da das Gesetz eine Beschränkung auf verbundene Dienste vorsieht.

Um faktische Probleme bei Herausgabeverlangen zu vermeiden, wird der Kreis der Verpflichteten noch enger gezogen: Daten herausgeben müssen nur Dateninhaber, „bei denen sich diese Daten befinden“ (Art. 14 DA). In der englischen Sprachfassung heißen diese (erneut zirkulär) „data holders […] which hold those data“. Legt man diese Formulierungen so aus, dass es auf die physische (unmittelbare) Verfügungsgewalt ankommt (wenngleich dies nicht wirklich eindeutig ist), so ergibt sich eine mögliche Gesetzeslücke: Häufig sind die Inhaber unmittelbarer Gewalt datenschutzrechtlich Auftragsverarbeiter nach Art. 28 DSGVO. Diese sind jedoch nicht Dateninhaber (s. ErwGr 22 Data Act). Die Auftragsverarbeiter wären

dann jedoch mangels ihrer Stellung als Dateninhaber nicht verpflichtet nach Kapitel V. Die Dateninhaber wiederum könnten ihre Pflichten nach Kapitel V umgehen, indem sie die Datenspeicherung ausgliedern. Dass ein derartiges Ergebnis nicht durchgreifen kann, ist bereits unter effet utile-Gesichtspunkten evident. Ein Gericht könnte dies auf verschiedene Art und Weise lösen, etwa im Sinne einer Analogie (die in der Rechtsprechung des EuGH ohnehin der französischen Rechtstradition folgend eher als interprétation gilt und daher einer geringeren Anwendungsschwelle unterliegt als die klassische Analogie im deutschen Recht). Vermutlich werden Gerichte letztlich– der datenschutzrechtlichen Logik folgend – Handlungen von Auftragsverarbeitern schlicht dem Dateninhaber zurechnen und den Dateninhaber entsprechend doch als einen solchen verstehen, bei dem sich die Daten befinden. Angesichts der hohen Relevanz der Datenherausgabeverlangen für die öffentliche Hand ist Dateninhabern jedenfalls davon abzuraten, auf dem Wege der Ausgliederung zu versuchen, sich ihrer Pflichten zu entledigen. Dies würde mit hoher Wahrscheinlichkeit im Ergebnis nicht gelingen.

Innerhalb der verpflichteten Dateninhaber gelten für Kleinst- und Kleinunternehmen noch einmal besonders enge Voraussetzungen einer solchen Pflicht: insbesondere muss ein öffentlicher Notstand vorliegen und die Daten dürfen nicht auf andere Weise unter gleichen Bedingungen gleich wirksam beschafft werden können (ErwGr 63 a.E.).

Insgesamt verfolgt Kapitel V ein gestuftes Konzept, das sich wie folgt darstellt:

Herausgabepflichten bei öffentlichem Notstand

Eine besonders weite Pflicht zur Übermittlung von Daten besteht im Falle eines „öffentlichen Notstands“. Dieser öffentliche Notstand hat drei Voraussetzungen (Art. 2 Nr. 29 Data Act):

- Eine zeitlich begrenzte Ausnahmesituation
- Negative Auswirkungen auf die Bevölkerung sowie das Risiko schwerwiegender und dauerhafter Folgen für die Lebensbedingungen oder wirtschaftliche/finanzielle Stabilität
- Die amtliche Feststellung und Ausrufung der Ausnahmesituation

Der Unionsgesetzgeber hatte damit klar die „Corona-Krise“ vor Augen und die damit einhergehenden Herausforderungen, etwa was die Nachverfolgung von Infektionsketten (und möglicherweise auch Informationen zu Impfungen und durchgeführten Tests) anbelangt. Aber auch im Zuge anderer Krisen wie umfassender Cybersicherheitsvorfälle, Energiekrisen, Naturkatastrophen oder Tierseuchen werden diese Regelungen künftig sicherlich Relevanz entfalten.

Im Falle eines solchen öffentlichen Notstands müssen verpflichtete Dateninhaber den öffentlichen Stellen Daten jeder Art herausgeben, mithin Daten sowohl mit als auch ohne Personenbezug. Die Datenherausgabe muss sich zudem als „erforderlich“ erwiesen, um den Notstand zu bewältigen. Hinzu kommt, dass es für die öffentliche Stelle keine Möglichkeit geben darf, sich diese Daten unter gleichwertigen Bedingungen auf andere Weise rechtzeitig und wirksam zu beschaffen.

Die fehlende Möglichkeit, sich diese Daten auf alternative Weise zu beschaffen, zielt insbesondere auf den Erwerb auf dem freien Markt ab. Hierfür gilt wiederum eine Ausnahme für den (sehr speziellen) Sonderfall insofern, als der Erwerb von anonymen Daten auf dem freien Markt nicht als mildere Maßnahme erforderlich ist, wenn dies der Erstellung amtlicher Statistiken dient und der Erwerb solcher Daten nach nationalem Recht nicht zulässig ist. Der Sinn hinter dieser Ausnahmeregelung mag sich nicht völlig erschließen (beispielsweise, weshalb geringere Schwellen zur Heranziehung von anonymen Daten als für personenbezogene Daten gelten und warum überhaupt Statistiken eine Sonderstellung genießen sollen, noch dazu eine privilegierte). Die Ausnahme mag in der Praxis aufgrund ihres engen Anwendungsbereichs ein Nischendasein leben.

Ein weit offensichtlicheres Problem ist die Schwelle für die „Erforderlichkeit“, um den Notstand zu bewältigen ebenso wie das Erfordernis einer fehlenden Alternativbeschaffungsmöglichkeit. Im Hinblick auf ersteres erschiene es (aus dem deutschen Verwaltungsrecht entlehnt) naheliegend, der öffentlichen Hand eine Art „Einschätzungsprärogative“ zuzugestehen. Wenn eine erlangte Information sich im Nachhinein als weniger relevant als erhofft darstellt, wird dies das Herausgabeverlangen nicht rückwirkend rechtswidrig werden lassen. Dies liegt insbesondere vor dem Hintergrund nahe, dass die öffentliche Stelle den Informationsgehalt der angeforderten Daten erst nach ihrem Erhalt vollständig wird beurteilen können.

Im Hinblick auf die fehlende alternative Erwerbsmöglichkeit stellt sich die Frage, ob die öffentliche Stelle (i) jeden Preis zahlen muss und (ii) ein vorher ausgeschöpftes milderes Mittel auch die Verpflichtung des Dateninhabers nach einem Verwaltungsakt ist, der auf anderer Basis als dem Data Act ausgesprochen wurde.

Der Data Act selbst erwähnt in seinem ErwGr 64 als Alternativmöglichkeiten die „freiwillige Bereitstellung von Daten durch ein anderes Unternehmen“ oder die Abfrage einer öffentlichen Datenbank. Ersteres wird sicherlich in der Praxis schwerlich durchsetzbar sein, kann aber natürlich bei Großkrisen wie den Geschehnissen um die Corona-Pandemie doch praktisch relevant werden.

Im Hinblick auf akzeptable Kosten wird man sich – in Anlehnung an ErwGr 65 – sicherlich am „jeweiligen Marktkurs“ orientieren. Liegt eine solche Möglichkeit zum

Erwerb zu angemessen Preisen nicht vor, muss das in Anspruch genommene Unternehmen die Daten grundsätzlich bereitstellen.

Herausgabepflichten bei reiner Aufgabenerfüllung

Ein womöglich häufigerer Anwendungsfall des Data Acts betrifft die in Art. 15 Abs. 1 lit. b zweite Konstellation: Einbezogen sind nur anonyme Daten. Die Pflicht zur Datenbereitstellung ist daher ein Paradebeispiel für die viel diskutierte „Flucht ins Datenschutzrecht“, wonach die Vermengung mit personenbezogenen Daten (oder die weite Interpretation des Personenbezugs) dazu führen könnte, dass in einigen Konstellationen die Pflicht nach Art. 15 Abs. 1 lit. b Data Act entfallen könnte.

Der wesentlichste Unterschied zur vorigen Konstellation besteht darin, dass es keines ausgerufenen (und tatsächlichen) Notstands bedarf. Stattdessen reicht es aus, dass das Beschaffen der Daten erforderlich ist, um eine bestimmte im öffentlichen Interesse liegende Aufgabe zu erfüllen. Ein ausdrücklich genanntes Beispiel ist die Erstellung amtlicher Statistiken. Die Schwelle für die Verpflichtung, Daten herauszugeben, ist hinsichtlich des Zwecks daher sehr niedrig angesiedelt.

Möglicherweise, um dies wiederum einzugrenzen, hat der unionale Gesetzgeber das Erforderlichkeitskriterium sehr strikt konkretisiert. Anders als bei einem Notstand muss die öffentliche Stelle „alle anderen ihr zur Verfügung stehenden Mittel ausgeschöpft“ haben, wie etwa den Erwerb der Daten auf dem freien Markt, die Inanspruchnahme bestehender Verpflichtungen zur Bereitstellung von Daten oder der Erlass neuer Rechtsvorschriften, die die rechtzeitige Verfügbarkeit der Daten gewährleisten könnten. Der Erwerb von Daten muss dabei als milderes Mittel nur zum „jeweiligen Marktkurs“ erfolgen (Erwägungsgrund 65). Ein solcher wird praktisch freilich häufig nicht allzu leicht zu ermitteln sein, da es oft um eine sehr spezielle, noch dazu von Zeitdruck geprägte Situation gehen wird.

Herangezogene Unternehmen, welche sich möglicherweise gegen ein Herausgabeverlangen zur Wehr setzen möchten, könnten an dieser Stelle anknüpfen und bei einem bestehenden Markt für derartige Daten ein Datenbereitstellungsverlangen zurückweisen.

Verfahren

Der Data Act regelt das Verfahren eines solchen Datenbereitstellungsverfahrens sehr umfangreich. Insbesondere muss die öffentliche Stelle darlegen, welche Daten verlangt werden (was sicherlich mit einigen Unsicherheiten einhergehen wird, wenn der öffentlichen Stelle nicht im Detail bekannt ist, über welche Daten der Dateninhaber verfügt), den Zweck und die Rechtsgrundlage der öffentlichen Aufgabe benennen, Fristen angeben, die Wahl des Dateninhabers begründen, Geschäftsgeheimnisse nach Möglichkeit beachten und vieles mehr (s. insb. Art. 17 Data Act). Falls diese Anforderungen nicht erfüllt sind, kann der Dateninhaber ein Herausgabeverlangen ablehnen (Art. 18 Abs. 2 Data Act).

Interessanterweise muss der Dateninhaber Datensätze anonymisieren, sofern die öffentliche Hand die Personenbezüge nicht benötigt. Falls dies doch der Fall ist, muss der Dateninhaber die Daten grundsätzlich pseudonymisieren (Art. 18 Abs. 4 Data Act). Dies dürfte sich in der Praxis als durchaus herausfordernd darstellen, da insbesondere die Anonymisierung großer Datensätze erfahrungsgemäß weit über die maschinelle Entfernung etwa von Namen hinausgeht. Zudem stellt sich die Frage, ob Art. 15 Abs. 1 lit. b, der bereits initial nur anonyme Daten betrifft, die öffentliche Stelle dazu ermächtigt, die Herausgabe gleich welcher Daten zu verlangen unter der Prämisse, dass der verpflichtete Dateninhaber dann die Daten eben anonymisieren muss. Nach hier vertretener Ansicht ist dies nicht der Fall, da andernfalls die Unterschiede zwischen den Voraussetzungen und den Rechtsfolgen einer Pflicht verwischt würden. Stattdessen sind Daten mit Personenbezug nur im Fall eines Notstands betroffen. Diese Daten müssen dann jedoch vor der Herausgabe anonymisiert werden, wenn dies ausreicht, um den durch die öffentliche Stelle verfolgten Zweck zu erfüllen.

Im Fall einer Datenherausgabe bei einem öffentlichen Notstand müssen Daten grundsätzlich kostenlos herausgegeben werden. Die öffentliche Stelle kann den Beitrag des Dateninhabers jedoch auf dessen Ersuchen hin öffentlich anerkennen (Art. 20 Abs. 1 Data Act). Im Falle einer Heranziehung für die sonstige Aufgabenerfüllung können Dateninhaber eine „faire Gegenleistung“ verlangen, welche mindestens die entstandenen Aufwände erfasst, aber auch eine „angemessene Marge“. Die Höhe der Gegenleistung wird in erster Linie nicht etwa durch die öffentliche Stelle, sondern durch den Dateninhaber bestimmt. Die öffentliche Stelle kann, sofern sie hiermit nicht einverstanden ist, bei der für die Überwachung der Einhaltung des Data Acts zuständigen Aufsichtsbehörde Beschwerde einlegen (Art. 20 Abs. 5 Data Act).

Rechtsgrundlagen nach der DSGVO

Sofern die Herausgabeverlangen auch personenbezogene Daten umfassen (wie gezeigt, ist dies auf den Fall eines öffentlichen Notstands beschränkt), stellt sich die Frage nach der datenschutzrechtlichen Rechtsgrundlage. Wir haben uns zu der Frage, wann ein Konflikt zwischen den beiden Gesetzeswerken vorliegt, bereits umfassend in Teil 3 unserer Reihe zum Data Act geäußert. Insbesondere statuiert Art. 1 Abs. 5 S. 1 des Data Acts, dieser gelte „unbeschadet“ der DSGVO. Die DSGVO genießt daher etwas vereinfach ausgedrückt einen Anwendungsvorrang für den Fall eines Konflikts zwischen diesen beiden Gesetzen. Wann ein solcher Konflikt vorliegt, ist nicht immer eindeutig bestimmbar.

Nach hier vertretener Auffassung besteht in diesem Fall kein solcher Konflikt: Zwar legt Art. 6 Abs. 1 DSGVO ein grundsätzliches Verarbeitungsverbot im Hinblick auf personenbezogene Daten fest. Hierfür ist jedoch eine Reihe von Ausnahmen vorgesehen, wobei hier insbesondere Art. 6 Abs. 1 lit. c DSGVO einschlägig sein dürfte. Danach ist die Verarbeitung rechtmäßig, wenn sie zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, welcher der Verantwortliche unterliegt. Der Dateninhaber dürfte stets auch der datenschutzrechtlich Verantwortliche sein und damit der Pflicht zur Herausgabe nach dem Data Act unterfallen. Ein Konflikt liegt nach hier vertretener Auffassung nicht vor, da die DSGVO selbst die Ausnahme von ihrer Grundregel vorsieht. Sofern eine Verpflichtung nach Art. 15 Abs. 1 lit. a Data Act für den Fall eines öffentlichen Notstands vorliegt, wird man daher datenschutzrechtlich eine Rechtfertigung nach Art. 6 Abs. 1 lit. c DSGVO annehmen können.

Sanktionen und praktische Bedeutung

Wie bei den übrigen Bestandteilen des Data Acts gilt auch hier, dass die Höhe der Sanktionen abseits der recht abstrakten Anforderungen des Data Acts („wirksam, verhältnismäßig und abschreckend“) noch nicht absehbar ist. Das deutsche Gesetz zur Konkretisierung einiger Inhalte existiert noch nicht. Jedenfalls dürfen auch bei Verstößen im Hinblick auf das hier relevante Kapitel V die Datenschutz-Aufsichtsbehörden Geldbußen nach der DSGVO „innerhalb ihres Zuständigkeitsbereichs“ verhängen.

Praktisch wird es spannend sein, zu sehen, wie die öffentliche Hand von ihren neuen Kompetenzen Gebrauch machen wird. Dies gilt insbesondere vor dem Hintergrund der recht niedrigen Schwelle, wonach es für die Herausgabe anonymer Daten im Hinblick auf den Zweck ausreicht, dass die öffentliche Stelle irgendeine ihr übertragene Aufgabe verfolgt.

Unternehmen, die entsprechend herangezogen werden, sollten ihr weiteres Vorgehen insbesondere davon abhängig machen, wie schützenswert ihre Daten sind. Sie verfügen jedenfalls über einige Möglichkeiten, sich zu verteidigen, insbesondere, durch eine genaue Prüfung, ob das Verfahren eingehalten wurde. Ratsam ist es zudem, Geschäftsgeheimnisse als solche zu bezeichnen, damit diese nicht durch die öffentliche Stelle offengelegt werden (Art. 19 Abs. 3 Data Act). Da im Fall eines Notstands zudem häufig keine Zeit für eine aufwändigere rechtliche Prüfung bestehen wird, empfiehlt es sich auch vor diesem Hintergrund (wie allerdings ohnehin angesichts diverser Verpflichtungen aus der DSGVO und dem Data Act), eigene Datenbestände im Hinblick auf Personenbezüge, Geschäftsgeheimnisse etc. bereits vorab zu klassifizieren.

Wie bei anderen Teilen des Data Acts auch, bleibt es bei den Zugriffsrechten der öffentlichen Hand spannend, zu sehen, wie relevant die neuen Regelungen werden.

6. Der Dateninhaber und der Nutzer als Zentralfiguren der Datenverordnung

Die „IoT-bezogenen“ Rechte und Pflichten des Data Acts bestehen insbesondere zwischen dem „Dateninhaber“ und dem „Nutzer“. Das Gesetz zeigt sich bei deren Definition sehr vage und missverständlich. Wir erläutern, wie diese beiden Zentralfiguren rechtssicher erfasst werden können.

Die Datenverordnung („DVO“) besteht aus verschiedenen Kapiteln, die nur teilweise sachlich miteinander zusammenhängen. Ein wichtiges Rechtssubjekt in mehreren dieser Kapitel der DVO ist der sogenannte „Dateninhaber“. Das Verständnis um die Identität des Dateninhabers ist deshalb zentral, um den personellen Anwendungsbereich wichtiger Teile der DVO zu bestimmen. Dies betrifft insbesondere die sog. „IoT-Regelungen“ in Kapitel II (und hiermit korrespondierend Kapitel III), aber auch Bestimmungen zur Herausgabe von Daten an öffentliche Stellen in Kapitel V DVO.

Im Rahmen der Ansprüche auf Herausgabe von Daten aus vernetzten Produkten und verbundenen Diensten ist gewissermaßen der „Gegenspieler“ des Dateninhabers der „Nutzer“. Auch dessen korrekte Identifikation ist wichtig und kann im Einzelfall (und insbesondere präventiv bei der Erarbeitung von Prozessen) durchaus herausfordernd sein. Eine besondere Schwierigkeit besteht zudem, wenn Gegenstand von Herausgabeverlangen auch personenbezogene Daten sind und diese nicht (nur) Informationen über den Nutzer, sondern (auch) über weitere betroffene Personen enthalten. Um diesen Herausforderungen gewachsen zu sein, empfiehlt es sich, für die eigenen vernetzten Produkte und verbundenen Dienste bereits frühzeitig die relevanten Personengruppen zu identifizieren.

Die Identifizierung des Dateninhabers

Das Gesetz definiert den Dateninhaber (englisch: „data holder“) in Art. 2 Nr. 13 DVO als „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“.

Diese Definition ist leider in verschiedener Hinsicht missglückt und bringt deshalb wenig Klarheit:

Grundsätzliche Logik der Definition

Recht offensichtlich enthält die Definition einen Zirkelschluss: Zusammengefasst ist Dateninhaber, wer nach der Datenverordnung (oder einem anderen Gesetz) verpflichtet ist, Daten bereitzustellen. Eine solche Verpflichtung ergibt sich insbesondere aus Art. 4 und 5 DVO. Diese Normen knüpfen auf Tatbestandsebene jedoch wiederum an den Dateninhaber an, dessen Definition ja aber gerade geprüft wird. Im Grunde sagt die Definition damit, man sei Dateninhaber, wenn man Dateninhaber ist und Daten herausgeben muss. Hiermit ist also wenig Klarheit gewonnen.

Beschränkung auf verbundene Dienste

Außerdem schließt die Definition mit einer wenig sinnvollen Beschränkung auf Daten, welche der Dateninhaber „während der Erbringung eines verbundenen Dienstes“ gewonnen hat. Der Wortlaut des Gesetzes klammert damit überraschenderweise solche Daten aus, die der Dateninhaber beim Einsatz eines vernetzten Produkts abgerufen oder generiert hat.

Nimmt man nur den Wortlaut des Gesetzes zum Maßstab, würde der Kern der „IoT-Regelungen“ aus Art. 4 und 5 DVO leerlaufen, soweit dieser ganz wesentlich die Herausgabe von „Produktdaten“ i.S.d. Art. 2 Nr. 15 durch den Dateninhaber zum Gegenstand hat. Bei diesen handelt es sich jedoch um Daten aus vernetzten Produkten. Wenn die Dateninhaberschaft jedoch ausschließlich an Daten aus verbundenen Diensten anknüpft, wären die Pflichten zur Herausgabe von Produktdaten gegenstandslos, weil sie keinen Adressaten hätten – es gäbe insoweit nie einen Dateninhaber. Hierbei kann es sich nur um einen redaktionellen Fehler des Gesetzgebers handeln, den der EuGH vermutlich im Wege einer „Korrektur“ des Gesetzes auflösen würde. Das Gesetz ist deshalb wohl so zu lesen, dass auch Produktdaten ein Unternehmen zum Dateninhaber machen können.

Interessant wäre dann gleichwohl der mögliche Anknüpfungspunkt einer Korrektur, und zwar dahingehend, auf welchen Vorgang mit Produktdaten es ankäme (also was die Entsprechung zur „Erbringung eines verbundenen Dienstes“ wäre). Sinnvollerweise wäre dies jedenfalls nicht die „Herstellung“ eines vernetzten Produkts, da dabei typischerweise (noch) keine Nutzerdaten generiert werden. Denkbar wäre es, darauf abzustellen, welche Person außer dem Nutzer und ggf. dem Datenempfänger nach Art. 5 DVO Produktdaten aus dem vernetzten Produkt kontrolliert (zu letzterem sogleich). Das Gesetz wäre dann beispielsweise wie folgt zu ergänzen/ zu lesen: „Dateninhaber [ist] eine […] Person, die nach […] Rechtsvorschriften berechtigt oder verpflichtet ist, Daten zu nutzen und bereitzustellen, die sie während der Erbringung eines verbundenen Dienstes abgerufen oder generiert hat oder über die sie (im Falle von Produktdaten) die Kontrolle ausübt“.

Eine rechtssichere Identifizierung des Dateninhabers ist damit nach dem Gesetzeswortlaut in seiner gegenwärtigen Fassung allein schwerlich möglich. Dies ist ein Ärgernis für die Rechtsanwender, weil damit Unsicherheiten einhergehen. Zugleich bieten sich gewisse Verteidigungsmöglichkeiten für den Fall, dass man vermeintlichen Pflichten einer Dateninhaberschaft aus dem Weg gehen möchte.

Position der Kommission

Die Kommission betont in ihren FAQ vom 3. Februar 2025 (Version 1.2), typischerweise seien Hersteller vernetzter Produkte auch Dateninhaber. Es sei jedoch auch möglich, diese Eigenschaft über ein Outsourcing vertraglich auf einen Dritten zu verlagern.

Als entscheidend für die Frage der Dateninhaberschaft wird nicht die Frage angesehen, wer die Hard- oder Software hergestellt hat, sondern wer den Zugang zu den ohne Weiteres verfügbaren Daten kontrolliert.

Diese Klarstellung ist in Teilen durchaus hilfreich, wenngleich sie den Anwendungsbereich der Pflichten des Dateninhabers zu sehr verengt. Die Pflichten des Dateninhabers beziehen sich nämlich nicht nur auf „ohne Weiteres verfügbare Daten“, sondern auch darüber hinaus auf andere Daten (etwa in Kapitel V DVO – dort findet sich zudem noch die Rechtsfigur der „Dateninhaber, bei denen sich die Daten befinden“, in ihrer Intransparenz noch gesteigert durch die englische Sprachfassung „data holders […] which hold those data“.

Ergebnis der Anforderungen an die Dateninhaberschaft

Berücksichtigt man auch den zuletzt dargestellten Aspekt, lässt sich die Position der Kommission leicht korrigiert anwenden. Das Kernkriterium der Dateninhaberschaft ließe sich dann wie folgt fassen: Es kommt darauf an, welche natürliche oder juristische Person die Kontrolle über Daten jeder Art innehat. Dies erscheint zunächst sehr allgemein. Die notwendigen Einschränkungen des Anwendungsbereichs bestimmter Pflichten ergeben sich dann aus den jeweiligen konkreten Vorschriften (also beispielsweise durch Beschränkungen auf „Produktdaten“, „ohne Weiteres verfügbare Daten“ etc. sowie auf die Existenz eines „Nutzers“, gleichsam als Gegenpartei des Dateninhabers, ebenso etwa durch Beschränkungen bei Kleinst- und Kleinunternehmen gem. Art. 7 DVO).

Die oben erwähnte Position der Kommission, es sei möglich, die Dateninhaberschaft vertraglich „outzusourcen“, steht dem nicht entgegen. Insoweit kommt es insbesondere auch auf rechtliche Möglichkeiten und damit einen wichtigen Teilbereich der „Kontrolle“ an (die faktische Kontrolle war zwischenzeitlich Anknüpfungspunkt von Entwürfen für die DVO, dies wurde jedoch gestrichen). Eine vertragliche Gestaltung kann also die Kontrolle beeinflussen. Der rechtliche Teil der Kontrolle ist auch wichtig, um beispielsweise die Dateninhaberschaft einzelner Arbeitnehmer auszuschließen, die rein faktisch auf bestimmte Daten zugreifen können.

Ausnahme für Auftragsverarbeiter gemäß DSGVO

Das Zusammenspiel mit der Datenschutz-Grundverordnung (DSGVO) kann die Qualifikation als „Dateninhaber“ zusätzlich beeinflussen. ErwGr 22 DVO statuiert, dass Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DSGVO nicht als Dateninhaber zu verstehen seien. In diesem Lichte erscheint auch die oben skizzierte Position der Kommission sinnvoll, dass es auf die Kontrolle des Datenzugangs ankommt und nicht nur auf die rein faktische Verfügungsmacht, die häufig beim Auftragsverarbeiter liegen wird.

Dies stellt auch sicher, dass Dateninhaber sich nicht durch eine gezielte Allokation der datenschutzrechtlichen Rollen ihrer Pflichten aus der Datenverordnung entziehen können. Der Verantwortliche kann nämlich aufgrund seiner Weisungsbefugnis auf den Auftragsverarbeiter dahingehend einwirken, dass letzterer dem Nutzer oder dem Dritten (ggf. über den Verantwortlichen und Dateninhaber) Daten herausgibt.

Die Bestimmung des Nutzers

Der Nutzer ist häufig der Anspruchsgegner des Dateninhabers. Insbesondere kann er vom Dateninhaber die Herausgabe bestimmter Daten an sich selbst (Art. 4 DVO) oder einen Dritten (Art. 5 DVO) verlangen. Ohne einen Nutzer treffen den Dateninhaber diese Pflichten nicht. Ob es überhaupt Nutzer zu einem bestimmten Produkt oder Dienst geben kann und wer Nutzer ist, erweist sich daher als sehr relevant.

Rechte an vernetzten Produkten/ Inanspruchnahme verbundener Dienste

Das Gesetz definiert den Nutzer in Art. 2 Nr. 12 DVO als

„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 verbundenen Dienste in Anspruch nimmt“.

Dass es dabei nicht auf den Besitz im Sinne der §§ 854 BGB ankommen kann, liegt bereits aufgrund des unionsrechtlichen Charakters der DVO auf der Hand. In anderen Sprachfassungen wird auch nicht etwa – vergleichbar dem „Besitz“ – auf die tatsächliche Sachherrschaft über das vernetzte Produkt abgestellt, sondern wohl auf das Eigentum oder eher untechnisch ein „gehören“ (engl.: „[…] that owns a connected product“; franz: „appartenir“, span.: „poseer“).

Auch durch die Erwähnung der vertraglichen Rechteübertragung und die „Inanspruchnahme“ wird deutlich, dass man Nutzer nicht durch rein faktische Inbetriebnahme oder Nutzung wird. Stattdessen muss die Person über ein „stable right“ verfügen, wie es die Kommission in ihren FAQ ausdrückt (beispielsweise als Eigentümer oder Mieter eines vernetzten Produkts; sicherlich auch als Anspruchsberechtigter an einem hiermit verbundenen Dienst). Ausgeschlossen sind damit reine Gefälligkeitsverhältnisse.

Hinsichtlich der verbundenen Dienste ist die gesetzliche Formulierung der „Inanspruchnahme“ im Gleichklang mit den „stable rights“ an den vernetzten Produkten so zu lesen, dass nicht jede Person, die den verbundenen Dienst irgendwie nutzt, zum Nutzer im Sinne der Datenverordnung wird. Üblicherweise wird dies derjenige sein, der (häufig vertraglich) zur Nutzung des Produkts berechtigt ist. Bei einem Mietwagen beispielsweise, der mit einem verbundenen Dienst verknüpft ist, wären dies nicht sämtliche Mitfahrer, welche den Dienst vielleicht faktisch auch kurzzeitig bedienen, sondern eher nur der Mieter. Bei einem intelligenten Küchengerät mit mehreren möglichen Nutzeraccounts wären nach hier vertretener Ansicht hingegen auch die übrigen Account-Inhaber (und nicht nur der Eigentümer des Küchengeräts) berechtigte Nutzer, nicht aber beispielsweise Besucher im Haushalt, die den verbundenen Dienst einmalig ausprobieren. Wird ein Kartenterminal zur Abwicklung von Kartenzahlungen dem Betreiber eines Restaurants zur Nutzung überlassen, ist er der Nutzer, nicht aber die das Terminal zu Zahlung nutzenden Restaurantgäste. Hier wird es sicherlich einige Grenzfälle geben, die erst in der Rechtsprechung geklärt werden.

Territorialer Anknüpfungspunkt

Interessanterweise kommt es für die Anwendbarkeit der hier relevanten Bestimmungen der DVO darauf an, ob der Nutzer seinen (Wohn-)sitz in der Union hat (und nicht etwa auf den Sitz des Dateninhabers oder den Ort, an dem die Daten gespeichert sind).

Art. 1 Abs. 3 b DVO drückt sich hierbei recht lakonisch und wiederum nicht ganz eindeutig aus: „Diese Verordnung gilt für […] die Nutzer der […] vernetzten Produkte oder verbundenen Dienste in der Union“. Unklar ist, ob sich die Nutzer oder die Produkte und Dienste in der Union befinden müssen. Deutlicher wird dies in anderen Sprachfassungen (im Englischen.: „users in the Union of connected products or related services“, im Französischen: „aux utilisateurs dans l’Union“, etwas ungelenk hingegen im Spanischen: „los usuarios de la Unión“). Relevant für die Eröffnung des personellen Anwendungsbereichs ist also im Sinne des Marktortprinzips der Aufenthalt des Nutzers.

Die Kommission interpretiert dies in ihren FAQ so, dass es darauf ankomme, ob der Nutzer in der Union „established“ sei. Dies ist sicherlich sinnvoll, um reine Zufallsergebnisse zu vermeiden (etwa bei Flugreisen über das Unionsgebiet). Nach hier vertretener Auffassung bedarf es hierfür nicht eines Haupt(wohn-)sitzes, wohl aber irgendeiner ständigen Niederlassung/ irgendeines ständigen Wohnsitzes.

Mehrzahl an Nutzern

Es ist denkbar, dass ein vernetztes Produkt (oder ein verbundener Dienst) über mehrere Nutzer verfügt. Dies ist zum einen „nebeneinander“ möglich, etwa bei Familienmitgliedern, die ein intelligentes Küchengerät nutzen. Eine praktische Möglichkeit, in einer solchen Konstellation die richtige Bearbeitung von Nutzeransprüchen zu gewährleisten, besteht darin, einzelne Nutzeraccounts zuzulassen.

Denkbar ist eine Mehrzahl an Nutzern auch gleichsam vertikal „in der Kette“. Die Kommission bildet hierfür das Beispiel eines Mietwagenanbieters, der ein vernetztes Fahrzeug an einen Mieter übergibt. Der Fahrzeughersteller kann bei entsprechenden Kontrollmöglichkeiten als Dateninhaber fungieren. Der Mietwagenanbieter als Eigentümer (oder Leasingnehmer) des Fahrzeugs kann Nutzer sein. Der Mieter des Wagens kann ebenfalls Nutzer sein, da ihm vertraglich ein temporäres Recht eingeräumt wurde.

Interessant in einer derartigen Konstellation dürfte es sein, zu sehen, ob eine Person gleichzeitig Dateninhaber und Nutzer sein kann (hier wäre dies beim Mietwagenanbieter denkbar, wenn sowohl der Hersteller als auch der Mietwagenanbieter Zugriff auf dieselben Daten hätte, der Mietwagenanbieter aber eben auch das Eigentum am Fahrzeug erworben hat und damit Nutzer wurde). Wir halten eine solche Doppelrolle für durchaus denkbar. Welche Rolle „durchschlägt“, bemisst sich dann nach dem jeweiligen Gegenüber, also ob der Anspruchsgegner hinsichtlich derselben Daten selbst Dateninhaber oder Nutzer ist.

Interaktionen mit dem Datenschutzrecht

Der Nutzer ist nicht zwingend identisch mit der „betroffenen Person“ aus Art. 4 Nr. 1 DSGVO. Beispielsweise kann eine Person ein vernetztes Produkt erwerben. Dieses Produkt kann jedoch von anderen Personen (temporär) genutzt werden, etwa von Arbeitnehmern oder Familienmitgliedern. Diese werden nicht zwingend selbst zu Nutzern im Sinne der DVO. Entsprechend wichtig ist es, bei der Bearbeitung von Herausgabeansprüchen nicht nur den Nutzer als Anspruchsinhaber im Blick zu behalten, sondern auch mögliche (andere) betroffene Personen. Der Dateninhaber benötigt für die Herausgabe personenbezogener Daten betroffener Personen an eine andere Person eine Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO. In einer solchen Konstellation kann es sinnvoll sein, Daten zu anonymisieren oder gemischte Datensätze zu trennen, um sowohl der DVO als auch der DSGVO gerecht zu werden (s. ErwGr 7 DVO).

Ergebnis

Es ist durchaus herausfordernd, die Rollen der insbesondere an den Rechten und Pflichten der „IoT-Regelungen“ teilhabenden Parteien treffsicher zu bestimmen. Erschwert wird dies durch die wenig präzisen Definitionen in der DVO selbst. Sinnvollerweise stellt man bei der Identifizierung des Dateninhabers darauf ab, wer die tatsächliche und insbesondere rechtliche Kontrolle über Daten jeder Art ausübt. Die weitere Eingrenzung des Anwendungsbereichs der jeweiligen Pflicht ergibt sich dann aus der jeweils konkreten Norm (etwa hinsichtlich bestimmter Datenkategorien).

Der „Gegenspieler“ des Dateninhabers ist der Nutzer, der über ein „stable right“ an dem vernetzten Produkt verfügen muss (etwa das Eigentum oder eine Miete/Leasing) oder berechtigterweise den verbundenen Dienst in Anspruch nimmt. Auch hier bestehen noch einige Unklarheiten, etwa welchen Grad der Berechtigung und Kontinuität die „Inanspruchnahme“ eines verbundenen Dienstes haben muss. Im Zweifel ist Unternehmen hier zu einer eher weiten Interpretation zu raten, die jedoch wiederum ihre Grenzen haben muss, soweit die Daten Personenbezug aufweisen. Der Nutzer muss zudem im Unionsgebiet „established“ sein, um den Anwendungsbereich der Datenverordnung zu eröffnen.

Unternehmen, die beispielsweise IoT-Geräte oder mit deren Funktionen verbundene Apps anbieten, sollten frühzeitig klären, ob und wenn ja für welche Daten sie Dateninhaber sind und wer Nutzer ist. Hierdurch wird gewährleistet, dass sie von den Pflichten aus der DVO nicht überrascht werden, sondern diese innerhalb der gesetzlichen Fristen („unverzüglich“) umsetzen können. Außerdem empfiehlt es sich, in derartigen Datensätzen enthaltene Personenbezüge zu identifizieren und Prozesse zum Umgang mit Datenherausgabeverlangen bereits frühzeitig aufzusetzen. Letztlich mag es ein Ergebnis der Analyse sein, dass das eigene Unternehmen „Nutzer“ ist und selbst Ansprüche auf die Herausgabe von Daten nach der DVO hat, die es für datenbasierte Geschäftsmodelle nutzen kann.

7. Was sind eigentlich „ohne Weiteres verfügbare Daten“?

Für mehrere Ansprüche aus dem „IoT-Teil“ des Data Acts sind die „ohne Weiteres verfügbaren Daten“ besonders relevant. Dieser Artikel erklärt, wann solche Daten vorliegen und wofür dies relevant ist.

Die Datenverordnung („DVO“) verpflichtet in Art. 4 und Art. 5 Dateninhaber, unter bestimmten Voraussetzungen Daten an Nutzer oder – auf Verlangen des Nutzers – an Dritte herauszugeben. Diese Datenzugangsrechte des Nutzers gelten jedoch nicht für sämtliche Daten, die das jeweilige vernetzte Produkt oder der damit verbundene Dienst generiert. Stattdessen beschränken sich die Ansprüche auf die Herausgabe von „ohne Weiteres verfügbaren Daten“ (in der englischen Sprachfassung: „readily available data“).

Diese Daten sollten von Dateninhabern bereits im Vorfeld möglicherweise geltend gemachter Ansprüche herausgearbeitet werden, um die Ansprüche entsprechend der gesetzlichen Anforderungen „unverzüglich“ umsetzen zu können.

Das Gesetz definiert in Art. 2 Nr. 17 DVO ohne Weiteres verfügbare Daten als „Produktdaten und verbundene Dienstdaten, die ein Dateninhaber ohne unverhältnismäßigen Aufwand rechtmäßig von dem vernetzten Produkt oder verbundenen Dienst erhält oder erhalten kann, wobei über eine einfache Bearbeitung hinausgegangen wird“.

Diese Definition untergliedert sich im Wesentlichen in drei Teile:

1. Es muss sich um Produktdaten oder verbundene Dienstdaten handeln.
2. Der Erhalt der Daten muss rechtmäßig sein.
3. Der Aufwand, mit dem ein Dateninhaber diese Daten rechtmäßig erhalten kann, muss verhältnismäßig sein.

Produktdaten oder verbundene Dienstdaten

Die erste Voraussetzung bemisst sich nach eigenen Definitionen aus der Datenverordnung, nämlich nach Art. 2 Nr. 15 und 16 DVO. Bei Produktdaten handelt es sich um „Daten, die durch die Nutzung eines vernetzten Produkts generiert werden und die der Hersteller so konzipiert hat, dass sie über einen elektronischen Kommunikationsdienst, eine physische Verbindung oder einen geräteinternen Zugang von einem Nutzer, Dateninhaber oder Dritten – gegebenenfalls einschließlich des Herstellers – abgerufen werden können“.

Produktdaten beziehen sich daher immer auf „vernetzte Produkte“.

Bei „verbundenen Dienstdaten“ wiederum handelt es sich um „Daten, die die Digitalisierung von Nutzerhandlungen oder Vorgängen im Zusammenhang mit dem vernetzten Produkt darstellen und vom Nutzer absichtlich aufgezeichnet oder als Nebenprodukt der Handlung des Nutzers während der Bereitstellung eines verbundenen Dienstes durch den Anbieter generiert werden“.

Nach Erwägungsgrund 15 DVO umfassen beide diese Kategorien absichtlich aufgezeichnete oder solche Daten, die indirekt durch Nutzerhandlungen generiert werden, wie z. B. Daten über die Umgebung oder Interaktionen des vernetzten Produkts. Hierunter sollen Informationen fallen, die von Sensoren des (in der Regel IoT-)Geräts (bzw. „Produkts“ in der Terminologie des Gesetzes) automatisch generiert wurden und Daten, die z.B. den Hardwarestatus und Funktionsstörungen über eingebettete Anwendungen umfassen. Beispiele sind Daten über die Temperatur, Geschwindigkeit oder den Flüssigkeitsstand.

Demgegenüber fallen Informationen, die erst aus Daten abgeleitet werden und das Ergebnis zusätzlicher Investitionen in die Zuweisung von Werten oder Erkenntnissen aus den Daten sind, nicht unter die Termini „Produktdaten“ oder „verbundene Dienstdaten“. Ebenfalls sollen in bestimmtem Umfang Inhalte wie Texte oder Audioinhalte nicht unter Produktdaten fallen (s. ErwGr 16).

Rechtmäßigkeit des Erhalts

Als ohne Weiteres verfügbare Daten gelten nur solche Daten, auf die der Dateninhaber in rechtmäßiger Weise zugreifen kann.

Der Dateninhaber wird nicht durch das Gesetz beispielsweise in einen Vertragsbruch gezwungen. Für Dateninhaber bieten sich dadurch möglicherweise durchaus Gestaltungsspielräume. Wenn Dateninhaber auf bestimmte Daten faktisch zugreifen können, diese aber nicht unbedingt benötigen und künftige Ansprüche nach der Datenverordnung vermeiden möchten, wäre es eine Möglichkeit, den Datenzugriff vertraglich bereits auszuschließen.

Aber auch bei Verboten aus anderen Gesetzen als der Datenverordnung mag man unter bestimmten Umständen die Eigenschaft als ohne Weiteres verfügbares Datum verneinen. Dies gilt jedenfalls bei dem sehr praktischen Anwendungsbeispiel einer Überschneidung mit der Datenschutz-Grundverordnung. Sofern im Datensatz personenbezogene Daten enthalten sind, gilt nach Art. 4 Abs. 12 und Art. 5 Abs. 7 DVO bereits ausdrücklich, dass die personenbezogenen Daten nur bei Vorliegen der Voraussetzungen des Art. 6 Abs. 1 (und ggf. des Art. 9 Abs. 1) DSGVO herausgegeben werden dürfen. Dies bedeutet nicht nur im Umkehrschluss, dass die Herausgabepflichten nach Art. 4 und Art. 5 DVO nicht als eine gesetzliche Pflicht im Sinne des Art. 6 Abs.1 lit. c DSGVO zu verstehen sind. Sofern für den Zugriff des Dateninhabers kein Erlaubnistatbestand aus dem Katalog des Art. 6 Abs. 1 DSGVO einschlägig ist, wäre wohl auch bereits tatbestandlich das Vorliegen eines ohne Weiteres verfügbaren Datums zu verneinen.

Nicht durch den Wortlaut des Gesetzes gelöst ist die Frage des korrekten normenhierarchischen Ansatzes für die Beurteilung der Rechtmäßigkeit des Erhalts der Daten. Insbesondere wäre es denkbar, dass mitgliedstaatliches Recht den Erhalt der Daten beschneidet. Nach hier vertretener Auffassung würde es jedoch zu weit führen, nationalen Vorschriften insoweit Vorrang einzuräumen. Andernfalls könnte der einzelne Mitgliedstaat den Anwendungsbereich einer vollharmonisierenden Verordnung zu weit ausdefinieren. Relevant sind insoweit Verbote aus mindestens gleicher Rangordnung, also insbesondere solche des europäischen Sekundärrechts.

Verhältnismäßigkeit des Aufwands

Das im Einzelfall sicherlich interpretationsbedürftigste Tatbestandsmerkmal der ohne Weiteres verfügbaren Daten betrifft die Möglichkeit des Erhalts der Daten für den Dateninhaber „ohne unverhältnismäßigen Aufwand“.

Die deutsche Sprachfassung der Datenverordnung schreibt dabei recht missverständlich, es werde „über eine einfache Bearbeitung hinausgegangen“. Es ist bereits unklar, worauf sich dieses Satzende bezieht. Mehr Erkenntnis liefern insoweit andere Sprachversionen: „without disproportionate effort going beyond a simple operation“, „sans effort disproportionné allant au-delà d‘une simple opération“, „sin un esfuerzo desproporcionado que vaya más allá de una operación simple“.

Es handelt sich also nicht etwa um eine weitere Tatbestandsvoraussetzung für ohne Weiteres verfügbare Daten, sondern um eine (sprachlich verunglückte) Konkretisierung der Verhältnismäßigkeit, nämlich sinngemäß: Aufwand, der nicht lediglich in einem einfachen Arbeitsschritt besteht.

Was diese Anforderung im Einzelfall bedeutet, ist freilich nicht vollständig rechtssicher zu konturieren. Einige Anhaltspunkte lassen sich dennoch entnehmen:

- Daten, über welche der Dateninhaber bereits die Kontrolle hat und auf sie z.B. in eigenen Datenbanken zugreifen kann, werden im Regelfall als ohne Weiteres verfügbar anzusehen sein.

- Umgekehrt sind alle Daten, die vom Dateninhaber erst generiert werden müssen, nicht von den Ansprüchen erfasst. Der Dateninhaber muss vernetzte Produkte und verbundene Dienste nicht so verändern, dass neue Daten überhaupt entstehen. Entsprechend kann der Dateninhaber durchaus durch eigene Designvorstellungen den späteren Umfang möglicher Ansprüche nach der Datenverordnung beeinflussen.

- Wenn auf Daten beispielsweise nur direkt an einem Gerät selbst und nicht remote zugegriffen werden kann und ein solcher Zugriff am Gerät selbst in der Praxis kaum möglich ist (z.B. weil die Geräte nicht beim Dateninhaber, sondern bei einem Kunden des Dateninhabers belegen sind), wären die Daten in der Regel nicht ohne Weiteres verfügbar.

Die einzelnen Aspekte der Verhältnismäßigkeit (und damit letztlich einer Abwägung) sind dabei umfassend zu würdigen. Dies bedeutet, dass nicht nur rechtliche, sondern auch technische und wirtschaftliche Faktoren zu berücksichtigen sind.

Konsequenzen der Einordnung

Soweit Dateninhaber zu dem Schluss kommen, dass sie auf Produktdaten und/oder verbundene Dienstdaten rechtmäßig und mit angemessenem Aufwand zugreifen können, sollten sie diese Daten als solche „clustern“ und in einer internen Policy folgenden Besonderheiten zuordnen:

- Grundsätzlich sind diese Daten auf Betreiben des Nutzers an diesen oder an Dritte herauszugeben.
- Sofern die Daten Personenbezüge enthalten (was schon aus datenschutzrechtlichen Gründen nicht erst im Fall eines gestellten Anspruchs, sondern bereits vorab z.B. im Rahmen des Verarbeitungsverzeichnisses nach Art. 30 DSGVO herauszuarbeiten ist), dürfen diese nicht ohne Vorliegen einer Rechtsgrundlage aus dem Katalog des Art. 6 Abs. 1 DSGVO herausgegeben werden (s.o., Art. 4 Abs. 12 und Art. 5 Abs. 7 DVO). Sofern für den Datenzugriff durch den Dateninhaber keine datenschutzrechtliche Rechtfertigung greift, handelt es sich zudem tatbestandlich bereits nicht um ein ohne Weiteres verfügbares Datum.
- Eigene Nutzungen anonymer Daten sind auf die Inhalte des Vertrags mit dem Nutzer beschränkt (Art. 4 Abs. 13 DVO).
- Anonyme Daten dürfen an Dritte nur auf Basis eines Vertrags mit dem Nutzer bereitgestellt werden (Art. 4 Abs. 14 DVO).

Über Osborne Clarke

Osborne Clarke ist eine internationale Wirtschaftskanzlei mit über 2.800 Mitarbeiterinnen und Mitarbeitern an 26 Standorten weltweit, davon über 280 Anwältinnen und Anwälte in Berlin, Hamburg, Köln und München. Mit dem Anspruch „Helping you succeed in tomorrow’s world“, ausgeprägter Branchenkenntnis durch Vernetzung und herausragender Kompetenz in Themen der digitalen Transformation von Geschäftsmodellen, der Dekarbonisierung und rund um Urban Dynamics berät und vertritt Osborne Clarke Unternehmen und Unternehmer in allen praktisch relevanten Fragen des Wirtschaftsrechts.