12 | 2025

Zeitschrift für Immaterialgüter-, Informations- und Wettbewerbsrecht

Revue du droit de la propriété intellectuelle, de l'information et de la concurrence

Themenheft: Digitalisierung
Numéro spécial: numérisation

Aufsätze / Articles

Rechtsprechung / Jurisprudence

Helbing Lichtenhahn
AIPPI
IGE | IPI

David Rosenthal

Der EU Data Act

Obwohl der EU Data Act bereits seit dem 12. September 2025 grösstenteils anwendbar ist, stehen viele Unternehmen erst am Anfang seiner Umsetzung. Diese neue Säule der EU-Digital-Regulierung birgt dabei erhebliche Herausforderungen: Sie gewährt Benutzern von Geräten und dazugehörigen Diensten weitreichende Rechte an den Daten, die diese generieren. Wenn die Anbieter dieser Geräte keine Vorkehrungen getroffen haben, ist ihnen selbst die bisher oft selbstverständliche Nutzung dieser Daten neu zudem bussenbewehrt verboten. Dabei stellen sich in der Praxis vor allem in Bezug auf den Anwendungsbereich komplexe Fragen. Dieser Beitrag liefert erste Antworten.

Bien que le règlement sur les données de l'UE (Data Act) soit en grande partie applicable depuis le 12 septembre 2025, de nombreuses entreprises n'en sont qu'au début de sa mise en œuvre. Ce nouveau pilier de la réglementation numérique de l'UE pose des défis considérables: il accorde aux utilisateurs d'appareils et de services associés des droits étendus sur les données qu'ils génèrent. Si les fournisseurs de ces appareils n'ont pas pris de dispositions, l'utilisation de ces données, qui allait souvent de soi jusqu'à présent, leur est désormais interdite sous peine d'amende. Dans la pratique, cela soulève des questions complexes, notamment en ce qui concerne le champ d'application, auxquelles cette contribution apporte des réponses initiales.

I. Überblick

Wer die Verordnung (EU) 2023/2854,[1] kurz den «Data Act», verstehen will, muss sich zunächst bewusst werden, dass es sich nicht um einen monothematischen Erlass handelt. Vielmehr reguliert er unterschiedliche Digital-Themen, die teils nichts miteinander zu tun haben.

Der Data Act deckt im Wesentlichen folgende Punkte ab:

1. **Zugang zu Daten, die Produkte generieren (Kapitel II)**: Generiert ein Produkt oder eine damit verbundene Dienstleistung abrufbare Sensor- oder Nutzungsdaten, dann sollen die Benutzer freien Zugang zu diesen Daten erhalten und einen solchen auch Dritten (z.B. Anbietern von konkurrierenden Dienstleistungen für dieses Produkt) verschaffen können. Die Anbieter wiederum sind in ihrer eigenen Nutzung der Daten eingeschränkt.
2. **Verträge betreffend das Teilen von Daten (Kapitel III, Kapitel IV)**: Für Verträge, die ein gesetzlich vorgeschriebenes Teilen von Daten regeln (wie zum Beispiel im Falle von Kapitel II), gelten nach Kapitel III bestimmte inhaltliche Vorgaben, die für Fairness sorgen und Missbräuche verhindern sollen. Für alle Verträge, die den Austausch von Daten im B2B-Bereich regeln, definiert Kapitel IV schliesslich noch weitere Klauseln, die als missbräuchlich gelten und daher unwirksam sind.
3. **Datenzugang für den Staat (Kapitel V)**: In Notsituationen verpflichtet der Data Act bestimmte Unternehmen, die nach Kapitel II über von Produkten und Dienstleistungen gesammelte Daten verfügen, diese auf Verlangen Behörden, der Europäischen Kommission oder anderen EU-Einrichtungen herauszugeben.
4. **Wechsel von Cloud-Diensten (Kapitel VI)**: Um die Abhängigkeit vor allem von den grossen Cloud-Anbietern zu reduzieren (Vendor-Lock-in), versucht der Data Act Hindernisse für den Anbieterwechsel zu beseitigen. Er tut dies, indem er den Anbietern von Cloud- und ähnlichen Datenverarbeitungsdiensten vorschreibt, dass sie einen Anbieterwechsel innert kurzer Frist technisch und vertraglich erleichtern und Entgelte für solche Wechsel bis Januar 2027 abzuschaffen.
5. **Schutz vor ausländischen Behördenzugriffen (Kapitel VII)**: Die Anbieter von Cloud- und ähnlichen Datenverarbeitungsdiensten müssen einen angemessenen

David Rosenthal, lic. iur., Partner/Lehrbeauftragter, Zürich.

1 Verordnung (EU) 2023/2854 des Europäischen Parlaments und des Rates vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828 (Datenverordnung), abrufbar unter ‹eur-lex.europa.eu/eli/reg/2023/2854›, zuletzt abgerufen am 29. Oktober 2025. Der Erlass ist am 11. Januar 2024 in Kraft getreten. Sämtliche Verweise auf Gesetzesartikel und Erwägungsgründe beziehen sich in diesem Beitrag, soweit nicht anders vermerkt, auf den Data Act.

Schutz vor ausländischen Behördenzugriffen bieten. Die Regelung ergänzt in gewisser Weise die EU-Datenschutz-Grundverordnung **(DSGVO)**, die dies so ähnlich für Personendaten schon vorsieht.

6. **Interoperabilität für Datenräume (Kapitel VIII)**: Wo in der EU Plattformen für den Austausch von Daten betrieben werden, müssen diese nach dem Data Act bestimmten Vorgaben für den reibungslosen Datenaustausch genügen.

Dieser Beitrag beschäftigt sich nur mit dem ersten und zweiten Punkt. Es sind diese beiden Regelungsbereiche, die in der Praxis besondere praktische Relevanz haben und am meisten Unternehmen tatsächlich betreffen. Kapitel VI zum Cloud-Wechsel wird zwar in der Öffentlichkeit immer wieder zitiert, und es ist auch lobenswert ist, dass der EU-Gesetzgeber sich um Massnahmen gegen einen Vendor-Lock-in bei Cloud-Providern kümmert. Deren Wirkung dürfte in der Praxis aber nur sehr beschränkt sein, auch wenn sie für die «grossen» Anbieter gedacht sind. Die heutigen Lock-in-Effekte sind jedenfalls bei den grossen Cloud-Plattformen nicht auf lange Kündigungsfristen, die fehlende Exportierbarkeit von Daten oder Wechselentgelte zurückzuführen. Verantwortlich sind andere Faktoren wie der kundenseitige Wechselaufwand und ein Mangel an Alternativen oder dem, was als Alternative betrachtet wird. Auch ist eine Regelung, die selbst kleinen Anbietern von Cloud-Services verbietet, längere Vertragslaufzeiten vorzusehen, nicht immer kundenfreundlich. Sie droht zum Beispiel die Möglichkeit von Rabatten bei gewollter längerfristiger Bindung zu vereiteln. Kurze Kündigungsfristen erlauben zudem den Providern auch kurzfristige Vertragsänderungen zum Nachteil von Kunden, die faktisch an den Provider gebunden sind und diese daher «schlucken» müssen.

II. Grundkonzept des Datenzugangs

Im Zentrum des hier diskutierten Datenzugangsregimes des Data Acts stehen Geräte, die in ihrem Betrieb Daten sammeln und bei denen diese Daten von aussen irgendwie abgerufen werden können. Bei diesen Geräten kann es sich um Consumer-Produkte handeln (z.B. ein Fitnesstracker, der den Herzschlag misst oder die Schritte zählt), aber ebenso um industrielle Systeme (z.B. eine Fertigungsanlage, welche Sensordaten sammelt und manuelle Eingriffe protokolliert). Diese Geräte gelten als «vernetzte Produkte» *(connected products)*. Ebenfalls erfasst sind damit «verbundene Dienste» *(related services)*. Gemeint sind Online-Dienste, die mit diesen vernetzten Produkten kommunizieren können und irgendwie deren Funktionalität oder Verhalten beeinflussen (z.B. indem sie bei einem Fahrzeug aus der Ferne die Klimaanlage einschalten können).

Wer solche vernetzten Produkte oder verbundenen Dienste verkauft oder vertraglich zur Verfügung stellt bzw. erbringt, muss diese so ausgestaltet haben, dass die abrufbaren, nicht veredelten Daten (z.B. Messwerte, Nutzungsaktivitäten) auch den Nutzern *(user)* zur Verfügung stehen – und zwar kostenlos, umfassend und möglichst direkt (Art. 3 (1)). Dies heisst, solche Geräte und Dienste müssen so gestaltet sein, dass neu nicht mehr nur der Anbieter die Daten abrufen kann, sondern auch der Nutzer selbst einen Zugang zu allen Daten erhält, sei es über eine Kabel- oder Drahtlosschnittstelle direkt am Gerät, sei es über ein Self-Service-Portal im Internet (z.B. bei einer Smartwatch, die gar keinen Datenanschluss hat). Dies wird als «Access-by-Design» bezeichnet. Hinzu kommt eine vorvertragliche Informationspflicht betreffend die wichtigsten Angaben zu diesem Zugang (Art. 3(2) und 3(3)). Diese Pflichten treffen nicht nur den Hersteller, sondern jeden in der Kette, der das Produkt oder den Dienst weiterverkauft oder vertraglich zur Verfügung stellt bzw. anbietet, und sie gelten auch im B2B-Verhältnis.

Unabhängig davon definiert der Data Act die Rolle des sog. Dateninhabers *(data holder)*. Gemeint sind jene, die im Rahmen eines Vertrags (mit dem Nutzer) über Daten der vernetzten Geräte oder verbundenen Dienste verfügen, wie z.B. der Anbieter eines solchen Dienstes oder derjenige, der diese Daten im Rahmen von Wartungsdiensten benötigt. Der Hersteller des Produkts kann, muss aber kein Dateninhaber sein.

Wer als Dateninhaber gilt, hat diverse Zusatzpflichten. Konkret muss er im Wesentlichen drei Dinge beachten:

- Er muss den Nutzern die ihm zugänglichen Daten auf Nachfrage kostenlos ebenfalls zugänglich machen, soweit sie nicht schon selbst Zugang dazu haben (Art. 4);
- Er muss auf Wunsch der Nutzer die Daten auch Dritten zugänglich machen, also beispielsweise Firmen, die mit diesen Daten ein Geschäft betreiben oder die für ein Gerät in Konkurrenz zum Hersteller Wartungsdienste anbieten und daher etwa Nutzungs- und Sensordaten des Geräts brauchen (Art. 5);
- Er darf die Daten nur für eigene Zwecke (z.B. Verbesserung seiner Produkte oder KI-Trainings) nutzen oder sie an Dritte weitergeben, soweit und solange dies vertraglich mit dem Nutzer so vereinbart worden ist (Art. 4(13)).

Die ersten beiden Punkte sind im Data Act etwas ausführlicher geregelt, um etwaige Geheimhaltungs- und weitere Interessen der Dateninhaber, der Nutzer und allfälliger Dritter zu schützen. Alle drei Punkte können und werden typischerweise vertraglich näher geregelt; es gibt hierzu bereits Entwürfe von Modellverträgen, die allerdings von beschränkter Tauglichkeit sind – die Europäische Kommission hat zum Zeitpunkt dieses Beitrags entsprechende Vorlagen noch nicht geliefert. Zudem sieht der Data Act noch gewisse Beschränkungen vor, um missbräuchliche Regelungen in solchen Verträgen zu verhindern.

Ausser der Pflicht nach Art. 3(1) zur Öffnung der Schnittstellen von vernetzten Produkten und verbundenen Diensten punkto Datenzugang für Nutzer sind all diese Bestimmungen seit dem 12. September 2025 auf Produkte und Dienste anwendbar, die in der EU auf den Markt gebracht oder dort bereitgestellt wurden; die Pflicht zum «Access-by-Design» ist erst ab dem 12. September 2026 anwendbar (Art. 50).

Dementsprechend ist der Data Act auch für alle Schweizer Unternehmen von Relevanz, die in den EU-Markt

exportieren, auch wenn seine Sanktionen – analog zur Situation unter der DSGVO – auf Schweizer Boden rechtlich nicht vollstreckt werden können. Wie es sich mit den Ansprüchen der Nutzer verhält, ist weniger klar. Hier kann mit guten Gründen vertreten werden, dass es sich im Sinne des Data Act um zivilrechtliche Ansprüche handelt, die letztlich Ausfluss einer Vertragsbeziehung in Bezug auf das vernetzte Produkt oder den verbundenen Service sind, die diesfalls wie andere Zivilansprüche auch in der Schweiz durchgesetzt werden könnten – analog der Situation unter der DSGVO. Abschliessend geklärt ist diese Frage noch nicht.

In der EU jedenfalls können Ansprüche nach dem Data Act über Streitbeilegungsdienste, Gerichte und Beschwerden bei den Aufsichtsbehörden durchgesetzt werden (die in manchen Mitgliedsstaaten noch gar noch nicht benannt oder bereit sind); unzulässige Klauseln können unwirksam sein, und hohe Geldbussen sind ebenfalls möglich. Bei Letzteren lehnt sich der Data Act in Bezug auf die Verletzung der hier relevanten Kapitel II (Art. 3–7) und Kapitel III (Art. 8–12) an den Bussenrahmen der DSGVO an (Art. 40 (4)), der bis zu 4% des weltweiten Jahresumsatzes oder EUR 20 Mio. vorsieht. Für weitere Verstösse gegen den Data Act müssen die Mitgliedsstaaten ihre eigenen Bussenkataloge definieren, was bisher erst teilweise geschehen ist.

Das Grundkonzept mag auf den ersten Blick einfach erscheinen. In der Praxis stellen sich aber vor allem viele Abgrenzungsfragen in der praktischen Umsetzung. Auf einige davon gehen wir nachfolgend ein. Juristische Lehre und Behördenpositionen zum Data Act gibt es allerdings noch kaum, was die Sache nicht einfacher macht.

III. Vernetzte Produkte und ihre Anbieter

Der Data Act gilt nur, wenn ein vernetztes Produkt oder ein verbundener Dienst vorliegt. Zwar ist immer wieder davon die Rede, dass es um das «Internet der Dinge» (*internet-of-things*, kurz «IoT») geht, aber der Data Act fasst viel weiter.

Erfasst ist jedes (fertig hergestellte) Gerät, das Daten über seine Nutzung oder seine Umgebung (z.B. GPS-Position, Temperatur) sammelt und bei welchem diese Daten über einen elektronischen Kommunikationsdienst, eine physische Verbindung oder einen geräteinternen Zugang von aussen abrufbar sind(Art. 2 Ziff. 5).[2] Es gibt zwar eine Ausnahme in der Legaldefinition für Geräte, deren Hauptfunktion die Speicherung, Verarbeitung oder Übertragung von Daten ist, doch gilt diese nur, wenn diese Aktivitäten im Namen einer anderen Partei als dem Nutzer erfolgen, was die Ausnahme in vielen Fällen nutzlos macht, da nach dem Anwendungszweck unterschieden werden muss.[3]

Das Produkt muss in der EU in Verkehr gebracht worden sein; ob es danach ausserhalb der EU benutzt wird, spielt keine Rolle (d.h. die Ansprüche nach Data Act bestehen trotzdem), ebenso umgekehrt nicht, dass ein ausserhalb der EU verkauftes, vermietetes oder verleastes Produkt in der EU benutzt wird (Ansprüche nach Data Act entstehen nicht, jedenfalls solange es nicht in der EU weitervermietet würde).[4]

Beispiele für vernetzte Produkte sind Smartwatches, einige moderne Autos (weil sie Leistung, Fahrverhalten, Umgebung ständig überwachen und diese Daten abrufbar sind), intelligente Kühlschränke (wenn sie z.B. Daten über Inhalt, Temperatur oder Nutzung erfassen und diese Angaben übermitteln können), Industrieroboter in einer Fertigungsstrasse (z.B. mit Daten über Betriebstemperatur, Funktionsstörungen oder ausgeführte Zyklen, um z.B. Wartungsbedarf vorherzusagen) oder smarte Thermostate (mit Daten über Raumnutzung oder Temperatur zur Steuerung der Heizleistung).[5] Kein vernetztes Produkt wäre hingegen ein einfaches digitales Thermometer, weil es zwar Daten erfasst und anzeigt, aber diese nicht über einen elektronischen Kommunikationsdienst, eine Verbindung oder geräteinternen Zugang abrufbar sind. Auch ein USB-Stick wäre nicht erfasst (er erhebt keine Daten über seine Nutzung oder Umgebung, sondern dient nur der Datenspeicherung), ebenso nicht ein Gerät, das Daten oder Signale lediglich weiterleitet. Bei einem Server liegt hingegen ein vernetztes Produkt vor, weil er zwar der Datenspeicherung im Auftrag Dritter dienen kann (Ausnahme von Art. 2(5)), dies aber nicht per se die Hauptfunktion eines solchen Geräts ist, da es vom Nutzer ebenso gut für eigene Speicherzwecke eingesetzt werden kann; Server weisen zudem die Merkmale anderer vernetzter Produkte auf (über eine entsprechende API kann z.B. die Prozessortemperatur abgerufen werden).

Ein weiteres Beispiel sind spezialisierte Laboranalysegeräte, die zwar primär Daten für den Nutzer verarbeiten, aber auch Betriebsdaten wie Temperatur oder Wartungszyklen erfassen und über eine Schnittstelle (z.B. USB oder Netzwerk) zugänglich machen; sie fallen ebenfalls unter die Definition der vernetzten Produkte. Die Anwendbarkeit des Data Act wird bei solchen «gemischten» Geräten über die Frage der Produktdaten (siehe nachfolgend) gesteuert, d.h. es muss geprüft werden, ob solche abrufbar sind, auch wenn das Gerät darüber hinaus noch viele andere Daten verarbeitet, die nicht erfasst sind.

Bei vernetzten Produkten muss ein Hersteller aufgrund der Pflicht zum «Access-by-Design» künftig nur, aber immerhin, dafür sorgen, dass alles, was er oder ein Dritter an vom Data Act erfassten Daten abrufen kann (was diese Daten sind, dazu sogleich), in Zukunft auch der Nutzer selbst abrufen und verarbeiten kann (Art. 3(1)). Der Nutzer muss also in Bezug auf den Zugang zu vom Gerät produzierte Daten gleichberechtigt sein. Verlangt wird, dass dieser Zugang «standardmässig […] einfach, sicher, unentgeltlich in einem

2 Also z.B. über ein Steckerverbindung am Gerät, Bluetooth oder einen Online-Dienst, der wiederum via Online-Verbindung mit dem Gerät in Verbindung steht und über diese Daten erhält.

3 Ein Server, den ein Cloud-Anbieter für seine Kunden betreibt, wäre kein vernetztes Produkt, wohl aber könnte es ein Server sein, den ein Unternehmen für sich betreibt.

4 Europäische Kommission, Frequently Asked Questions – Data Act, Version 1.3 vom 12. September 2025, abrufbar unter ‹digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act›, zuletzt abgerufen am 29. Oktober 2025, Frage Nr. 9.

5 Vgl. Erwägungsgrund 14.

umfassenden, strukturierten, gängigen und maschinenlesbaren Format und, soweit relevant und technisch durchführbar, direkt» möglich ist (ebd.). Das wäre in der Praxis zum Beispiel dann nicht der Fall, wenn das Gerät diese Daten verschlüsselt; der Anbieter müsste dem Benutzer den Schlüssel geben. Hat der Anbieter bisher ein proprietäres Format verwendet, muss er dies folglich anpassen. Der Anbieter muss auch erklären, was die Daten bedeuten und die für die «Auslegung und Nutzung dieser Daten erforderlichen Metadata» mitliefern. Wenn also ein Gerät über eine Datenschnittstelle verfügt, dann gehört eine entsprechende API-Dokumentation mit dazu. Hat der Anbieter das Gerät nicht selbst hergestellt, muss er sich die nötigen Informationen beschaffen und – etwa im Rahmen der Spezifikationen – künftig dafür sorgen, dass alle Produkte, die er wiederverkaufen oder sonst seinen Kunden vertraglich bereitstellen will, diese Vorgaben einhalten, weil er dafür selbst verantwortlich wird. Er kann sich nicht darauf berufen, dass der Hersteller das Access-by-Design nicht umgesetzt hat. Das ergibt sich indirekt aus Art. 3(1), welcher die Anforderungen an Produkte definiert, in Kombination mit Art. 3 (2), welcher die Informationspflichten über solche Produkte regelt und nicht nur für den Hersteller gilt, sondern auch für weitere Stellen in der nachgelagerten Lieferkette.

Das Erfordernis des «direkten» Zugangs meint, dass der Nutzer über die technischen Mittel verfügen kann, um auf die betreffenden Daten zuzugreifen, sie zu streamen oder herunterzuladen, ohne den Anbieter darum ersuchen zu müssen.[6] Vereinfacht gesagt: Er muss in einem Self-Service-Verfahren an die Daten gelangen können. Kein direkter Zugang besteht, wo jeweils ein Antrag auf Zugang gestellt werden muss, um an die Daten zu gelangen (ein solches Verfahren kann hingegen beim Datenzugang nach Art. 4 ff. vorgesehen sein). Hingegen gilt ein Zugang ebenfalls als direkt, wenn er online über einen Server des Anbieters in Selbstbedienung möglich ist (z.B. via Self-Service-Portal oder Online-API), auch wenn er nicht am Gerät selbst erfolgt. Der physische Speicherort der Daten ist für die Frage der Direktheit des Zugangs somit nicht entscheidend.[7] In der Praxis ist die Unterscheidung nicht so wichtig, da der Data Act den direkten Zugang nur verlangt, wo «relevant und technisch» durchführbar (Art. 3(1)), d.h. der Entscheid über das Design liegt bis zu einem gewissen Mass beim Hersteller.[8] Der Vorbehalt der Relevanz und technischen Durchführbarkeit kann theoretisch sogar dazu führen, dass Daten gar nicht zugänglich sind, falls sich für die Daten vernünftigerweise niemand interessiert; wir haben solche Fälle bisher allerdings nicht gesehen.

In der Praxis sehen wir bei der Erfüllung von Art. 3(1) nicht sehr viele Schwierigkeiten; meist verfügen die Geräte bereits über lokale Schnittstellen, oder der Datenzugang ist im Rahmen von verbundenen Dienstleistungen online vorgesehen.

Hingegen treffen wir immer wieder den Fall an, dass ein Anbieter nicht will, dass Nutzer über alle Daten frei verfügen können, weil z.B. Konkurrenten sie für ihre Zwecke zum Nachteil des Anbieters nutzen könnten (z.B. konkurrierende Angebote). Er möchte also den Kreis der verfügbaren Daten einschränken und geltend machen, dass gewisse Daten rein «interner» Natur sind. Eine solche Unterscheidung kennt der Data Act aber nicht. Einen Schutz für Geschäftsgeheimnisse bietet der Data Act beim Access-by-Design (anders als dem Dateninhaber) ebenfalls nicht. Das bedeutet, dass der Hersteller das Problem selbst entschärfen muss, entweder durch Verzicht auf bestimmte Daten oder indem er sie bereits im Gerät veredeln lässt, weil dann die Pflicht nicht mehr greift (siehe nachfolgend), oder durch eine vertragliche Regelung, die aber wohl nicht über das hinausgehen darf, was der Data Act für Dateninhaber an Schutz vorsieht (dazu weiter hinten) – geklärt ist diese Frage bisher nicht.

Eine weitere Herausforderung ergibt sich in der Praxis aus dem Umstand, dass vernetzte Produkte selbst andere vernetzte Produkte enthalten können: Ein Fahrzeug kann z.B. elektronische Steuergeräte, Batteriemanagementsysteme, Reifendrucksensoren oder In-Vehicle-Entertainment-Systeme enthalten, die ihrerseits vernetzte Produkte sind. Die genannten Pflichten gelten für alle Anbieter und Produkte in der Wertschöpfungskette. Wenn also der Anbieter des Batteriemanagementsystems die Daten für seine Zwecke nutzen will, muss er die Zustimmung des Nutzers haben (Art. 4(13)), wobei bereits an dieser Stelle nicht wirklich klar ist, wer der Nutzer im Sinne des Data Acts ist – der Anbieter, der das System verbaut, oder (auch) derjenige, der das Fahrzeug erworben oder gemietet hat. Es gibt Argumente für beides; der Umstand, dass die Daten der Komponente via den Datenbus im Fahrzeug über die Schnittstelle des Fahrzeugs von aussen abgerufen werden können, macht die Sache nicht einfacher. In der Praxis ist die Antwort nicht entscheidend: Hat der Fahrzeuganbieter den Zugang zu diesen Daten aus dem Betrieb, wird jedenfalls er zum Dateninhaber und vom Nutzer so oder so Zustimmung zur Nutzung und Weitergabe dieser Daten einholen müssen, d.h. er muss die Zustimmung so breit definieren, dass sie die Weitergabe auch an den Hersteller des Batteriemanagementsystems erfasst. Hat dieser einen vertraglichen Anspruch darauf, kann dieser je nach Interpretation gemäss der Legaldefinition selbst zum Dateninhaber werden, und das «Spiel» von Art. 4 ff. geht von vorne los; es wird hier aber auch vertreten, dass lediglich derjenige als Dateninhaber gilt, der mit dem Nutzer (hier vermutlich der Fahrzeughalter) einen Vertrag hat.

Eine vertragliche Regelung und ein Access-by-Design genügt wie bereits erwähnt nicht zur Einhaltung des Data Act. Hinzu kommt die Pflicht zur Vorabinformation des Nutzers. Sie setzt jeweils bei demjenigen an, der das Produkt einem Nutzer vertraglich zur Verfügung stellt, und sei es nur temporär zur Miete oder im Rahmen eines Leasings. Das Autohaus informiert beim Fahrzeugverkauf also die Mietwagengesellschaft, und diese muss wiederum jeden Mieter vorab über die am Gerät abrufbaren Daten informie-

6 Europäische Kommission, FAQ (Fn. 4), Frage Nr. 17.
7 Europäische Kommission, FAQ (Fn. 4), Frage Nr. 22.
8 Europäische Kommission, FAQ (Fn. 4), Frage Nr. 17.

ren (Art. 3(2)). Die Information darf generisch sein; erwartet wird nicht eine Anleitung, wie die Daten abrufbar sind. Es geht vielmehr darum, dem Nutzer aufzuzeigen, welche Daten von «seinem» Produkt erhalten werden können – und zwar vor Vertragsschluss. In der Praxis wird das über Hinweise in AGB, Offerten und Produktedokumentationen gemacht, die Verweise auf eine Website enthalten, auf der dann die produktespezifischen, vom Gesetzgeber verlangten Angaben abrufbar sind.

Fallstricke gibt es natürlich auch hier: Die Erwartung ist, dass diese Informationen jeweils auch Angaben über die Identität des Verkäufers, Vermieters oder Leasinggebers enthält; der Data Act unterscheidet nicht zwischen «first hand»- und «second hand»-Produkten.[9] Diese weiteren Stellen müssen sich also um eine eigenständige Information kümmern und können nicht bloss darauf vertrauen, dass der Hersteller informiert. Sie werden ihn aber von Vorteil dazu verpflichten, ihnen die für die Information nach Art. 3(2) nötigen Angaben zu liefern – nebst der Zusicherung einer Data-Act-konformen Gestaltung seiner Produkte. Ist für den Zugang zu Daten ein Online-Service erforderlich, werden sie sich auch diesbezüglich mit ihm absprechen müssen, damit ihren Kunden der Zugang gewährleistet ist, auch wenn diese keine direkte Vertragsbeziehung mit dem Hersteller haben.

IV. Erfasste und nicht erfasste Gerätedaten

Spätestens an diesem Punkt entsteht nach unserer Erfahrung das Bedürfnis, den Kreis der vom Data Act erfassten Daten und damit auch die Pflichten einzuschränken. Das ist durchaus möglich und empfiehlt sich auch.

Zunächst gelten die Pflichten nicht betreffend alle Daten, die vernetzte Produkte produzieren. Sie gelten grundsätzlich nur für sog. Produktdaten *(product data)*, was aus Art. 3 noch ausdrücklich hervorgeht, bei Art. 4 ff. aber immerhin aus dem Titel von Art. 4. Die Begriffsdefinition von Art. 2 Ziff. 15 ist leider ebenfalls nicht präzise. Aus ihr geht hervor, dass nur jene Daten gemeint sind, die auch tatsächlich zum Abruf von aussen gedacht sind. Wenn also ein Gerät intern irgendwelche Dinge protokolliert, diese aber in dieser Form nicht abrufbar sind (auch nicht für den Hersteller), dann sind es keine Produktdaten. Der Abruf muss zudem über den elektronischen Kommunikationsdienst, eine physische Verbindung oder einen geräteinternen Zugang erfolgen, d.h. die Anzeige auf einem Display genügt normalerweise nicht. Der Hersteller kann also entscheiden, welche Daten überhaupt in Frage kommen.

Doch auch nicht alle an sich abrufbaren Daten gelten als Produktdaten; der Wortlaut der Legaldefinition ist viel zu breit gefasst. Hier ist ein Blick in die Erwägungsgründe 15 ff. nötig:

- Erfasst sind nur jene (abrufbaren) Daten, die sich auf die **Leistung, Nutzung oder Umgebung** des Produkts beziehen und von diesem generiert werden.[10] Gemeint sind Daten, die durch die Nutzung des vernetzten Produkts entstehen, wie z.B. Daten über die Umgebung (in der Regel Messwerte von Sensoren, wie z.B. Temperaturen oder eine Geoposition) oder über Interaktionen mit dem vernetzten Produkt (z.B. die Gebrauchszeit oder die benutzten Funktionen). Erfasst sind auch Daten, die Fehlfunktionen oder den Status des Geräts betreffen, jedenfalls sofern sie vom Gerät generiert werden (unklar: Versionsnummer der aktuellen Firmware). Keine Rolle spielt, ob die Daten abgespeichert oder sogleich extern kommuniziert werden.
- Nicht erfasst sind hingegen aus solchen Daten **gefolgerte oder abgeleitete Informationen**, die das Ergebnis zusätzlicher erheblicher Investitionen des Herstellers des Geräts sind, insbesondere wo sie durch komplexe proprietäre Algorithmen erzeugt wurden. Der Data Act will Zugang zu den bei der Nutzung des Geräts anfallenden Rohdaten verschaffen, nicht aber veredelten Daten. Damit letztere vorliegen, muss ein gewisser Aufwand betrieben worden sein bzw. proprietäres Know-how zum Einsatz gekommen sein. Wenn der Spannungswert des Temperatursensors im Gerät zuerst in einen Temperaturwert umgewandelt wird, so gilt auch letzterer als Produktdatum. Wenn aus mehreren Temperaturwerten und anderen Angaben nach einem proprietären Algorithmus berechnet wird, wann das Gerät gewartet werden muss, dann gilt diese Information nicht als Produktdatum und muss weder für den Nutzer abrufbar noch unter Art. 4 ff. herausgegeben werden. Geschäftsgeheimnisse sind also für sich kein Ausschlusskriterium, aber die Verwendung solcher zur Veredelung unter Umständen schon. Unternehmen können also erwägen, Rohdaten bereits im Gerät durch komplexe proprietäre Algorithmen zu veredeln. Statt roher Sensordaten könnte das Gerät z.B. nur noch einen proprietären Diagnose-Code ausgeben, der bereits eine erhebliche Wertschöpfung mit sich bringt. Es liesse sich argumentieren, dass dieser Code kein Produktdatum mehr ist, sondern eine abgeleitete Information, die nicht unter die Herausgabepflicht fällt und, selbst wenn abrufbar, nicht erklärt werden muss, was er bedeutet.
- Nicht erfasst sind gemäss Erwägungsgrund 16 im Weiteren jene Daten, die **woanders gesammelt** und **lediglich zur Speicherung** oder weiteren Übermittlung an das Gerät übermittelt wurden und von dort wieder abgerufen werden können.[11] Ein Beispiel sind die Daten, die auf

9 Europäische Kommission, FAQ (Fn. 4), Frage Nr. 11.

10 Erwägungsgrund 15: «… Produktdaten bezeichnet Daten, die durch die Nutzung eines vernetzten Produkts generiert werden und die der Hersteller so konzipiert hat, dass sie von einem Nutzer, Dateninhaber oder Dritten – gegebenenfalls einschliesslich des Herstellers – aus dem vernetzten Produkt abgerufen werden können.…»; Erwägungsgrund 16: «… Diese Verordnung ermöglicht es Nutzern vernetzter Produkte, Folgemarkt-Dienste, Nebendienste und sonstige Dienste zu nutzen, die auf Daten basieren, die von in diese Produkte eingebetteten Sensoren erhoben werden, wobei die Erhebung dieser Daten von potenziellem Nutzen für die Verbesserung der Leistung der vernetzten Produkte ist.…».

11 Ob demnach im erwähnten Beispiel des Fahrzeugs, das Daten seiner Komponenten (wie z.B. der Steuereinheit oder des Batteriemanagementsystems) sammelt, diese Daten Produktdaten des Fahrzeugs sind oder nur der Komponenten, ist nicht klar. Es liesse sich vertreten,

einem Server gespeichert werden, damit sie später wieder abgerufen werden können, und zwar gleichgültig, ob dies für den Nutzer geschieht oder im Auftrag von Dritten.[12] Erhält ein intelligentes Fahrzeug jedoch Daten von einer intelligenten Strasse übermittelt, damit es diese für die Fahrzeugsteuerung verarbeiten kann und zeichnet es sie auf, sind diese Daten als Umgebungsdaten erfasst.

– Nach Erwägungsgrund 16 ebenso nicht erfasst sein sollen Inhalte, die als geistiges Eigentum geschützt sind oder für den menschlichen Konsum bestimmt sind. Der Data Act spricht generell von «**Content**», der nicht erfasst sein soll. Gemeint sind etwa multimediale Inhalte, Software oder von Menschen verfasste Texte. Doch auch hier gibt es Gegenbeispiele und es wird klar, dass selbst mit den Ausführungen der Erwägungen (und auch der FAQ der Europäischen Kommission)[13] nicht völlig klar ist, wo die Trennlinie verläuft. Wird ein Fotoapparat von einer Person genutzt, um damit eine Aufnahme zu machen, so ist das Bild kein Produktdatum, insbesondere nicht, weil es oft auch urheberrechtlich geschützt sein wird – in gewissen Rechtsordnungen sogar fast immer. Die Bilder der in einem modernen Fahrzeug verbauten Umgebungskameras gelten hingegen als Produktdaten, wobei das Kriterium der Konsumation durch einen Menschen hier gerade nicht schlüssig ist: Die Bilder dienen zwar einerseits dem Spurhalteassistenten, beim Einparken aber andererseits auch dem Fahrer.[14]

Ist ein Datum kein Produktdatum, kann der Zugang des Nutzers dazu beschränkt oder verweigert werden, z.B. durch Verschlüsselung oder vertragliche Nutzungsverbote. Im Rahmen von Art. 4 ff. muss es schlicht nicht herausgegeben werden. Es kann sich also lohnen, die einzelnen abrufbaren Daten einer Prüfung zu unterziehen oder allenfalls sogar durch besondere Algorithmen bereits im Gerät zu veredeln, damit sie der Konkurrenz nicht in die Hände fallen. Solche Massnahmen können aber auch ganz praktische Gründe haben: Wenn Zugang zu einem Datum gewährt werden muss (weil bisher zwar nicht der Nutzer, aber der Hersteller Zugang hatte, und sei es z.B. nur im Falle einer Wartung vor Ort), dann muss dem Nutzer auch erklärt werden, was es mit dem Datum auf sich hat, damit er es vernünftig nutzen kann. Allfällige Metadaten sind mitzuliefern. Das kann mit einigem Aufwand verbunden sein.

V. Verbundene Dienste

Dieselben Grundsätze gelten an sich auch für verbundene Dienste. In der Praxis ist hier eine der Herausforderungen, solche verbundenen Dienste überhaupt zu erkennen bzw. abzugrenzen gegenüber anderen Diensten. Einfacher als bei einem vernetzten Produkt ist hier immerhin, dass es weniger oft zu Kettenverhältnissen kommt bzw. weniger Stakeholder beteiligt sind: Während ein modernes Auto über den Handelskanal mehrfach seinen Eigentümer wechselt, wird der Online-Dienst, auf welches das Fahrzeug für sein Navi, sein Entertainment-System etc. zugreift, in der Regel immer vom Hersteller direkt erbracht. Ihn trifft dann auch die vorvertragliche Informationspflicht (Art. 3(3); sie ist etwas ausführlicher als bei einem vernetzten Produkt), wobei im genannten Beispiel nicht der Autokauf den Zeitpunkt der spätesten Information setzt, sondern die Aktivierung des Online-Dienstes typischerweise nach dem Verkauf des Fahrzeugs (auch wenn die Information vorgängig sinnvoller sein mag, weil dem Nutzer nach dem Kauf des Fahrzeugs kaum eine Wahl bleibt, ob er den Online-Dienst will oder nicht).

Der Hersteller des vernetzten Geräts und der Anbieter eines damit verbundenen Dienstes müssen nicht identisch sein; wesentlich für die Pflichten ist, wer den Dienst dem Nutzer in rechtlicher Sicht anbietet, d.h. mit ihm den entsprechenden Vertrag unterhält (derjenige, der den Dienst praktisch durchführt, wird vom Data Act nicht verpflichtet und gilt auch nicht als Dateninhaber, solange er die Daten nicht in eigener Verantwortung bzw. für eigene Zwecke nutzt).[15]

Als verbundener Dienst gilt jeder digitale Dienst «einschliesslich Software», der kein elektronischer Kommunikationsdienst ist, aber entweder bereits beim Kauf, der Miete oder dem Leasing so mit dem vernetzten Produkt verbunden ist, dass es ohne ihn eine oder mehrere seiner Funktionen nicht ausführen könnte, oder nachträglich vom Hersteller oder einem Dritten mit ihm verbunden wird, um die Funktionen des vernetzten Produkts zu ergänzen, zu aktualisieren oder anzupassen (Art. 2 Ziff. 6).

Erforderlich ist also

– ein zweiseitiger bzw. bidirektionaler Datenaustausch zwischen dem vernetzten Produkt und dem Dienstanbieter, und
– dass der Dienst die Funktionen, das Verhalten oder den Betrieb des vernetzten Produkts beeinflussen muss.[16]

Beispiele (vgl. dazu Erwägungsgrund 17):

– **Navigations-App des Autoherstellers**: Ein Dienst, der mit dem Infotainmentsystem des Autos verbunden ist, Daten austauscht (z.B. Fahrzeugposition) und Befehle an das vernetzte Produkt übermittelt, die dessen Funktionalität bzw. Verhalten beeinflussen (Anzeige der Routenführung auf dem Display des Fahrzeugs).
– **Software zur Fernsteuerung einer Smart-Home-Heizung**: Eine Anwendung, die es dem Nutzer ermöglicht, die Funktionen des vernetzten Produkts (Thermostat) aus

dass sie mit dem Einbau der Komponente zum Fahrzeug werden, aber ebenso, dass sie ein separates vernetztes Produkt bleiben (zumal die Komponente ja über eine eigene Schnittstelle verfügt), bei welchem der Zugang lediglich indirekt über die Fahrzeugschnittstelle sichergestellt wird. Genau genommen hätte dies Folgen für die Informationspflicht. In der Praxis wird hier aber nicht unterschieden; der Anbieter des Fahrzeugs wird typischerweise über alle Daten informieren, die abrufbar sind.

12 Insofern ist die Ausnahmebestimmung von Art. 2 Ziff. 5 praktisch irrelevant.
13 Europäische Kommission, FAQ (Fn. 4), Frage Nr. 10.
14 Europäische Kommission, FAQ (Fn. 4), Frage Nr. 6.
15 Insofern folgt der Data Act dem Datenschutzrecht: Verantwortlich ist der Controller, nicht der Processor; Auftragsbearbeiter gelten nicht als Dateninhaber (Erwägungsgrund 22).
16 Europäische Kommission, FAQ (Fn. 4), Frage Nr. 10.

der Ferne zu steuern, zu aktualisieren oder anzupassen, indem Daten und Befehle ausgetauscht werden.
- **Firmware-Update-Dienst für eine Drohne**: Ein vom Hersteller bereitgestellter Dienst, der die Software des vernetzten Produkts aktualisiert, um dessen Funktionen zu ergänzen oder anzupassen, was für den sicheren Betrieb unerlässlich sein kann.
- **Fitness-Tracking-Anwendung für eine Smartwatch**: Eine Software, die mit der Uhr verbunden ist, um die von ihr generierten Gesundheitsdaten zu verarbeiten, zu visualisieren und so die Funktionalität des vernetzten Produkts (der Uhr) für den Nutzer zu ergänzen (d.h. eine Funktion ausführen, die der Uhr zugerechnet wird, weil diese beim Verkauf als Teil der Uhr angepriesen worden ist). Das Beispiel zeigt, dass die Ausgestaltung und Vermarktung von vernetzten Produkten einen Einfluss darauf haben kann, was als verbundener Dienst gilt.

Kein verbundener Dienst wäre ein separater Versicherungsvertrag für ein Auto (reine Finanzdienstleistung; das wäre selbst dann kein verbundener Dienst, wenn die Prämie basierend auf Fahrzeugfahrdaten berechnet würde, die automatisch vom Fahrzeug übermittelt würden, da keine Befehle an das Fahrzeug erfolgen), ein Internetzugang (reine Bereitstellung von Konnektivität), ein Reparaturdienst für Haushaltsgeräte (der Dienst betrifft das Produkt, ist aber nicht damit verbunden), die Versorgung mit Strom (keine Kommunikation),[17] eine App, mit welcher von einem Gerät Informationen nur abgerufen werden können (bidirektionale Kommunikation, aber keine Beeinflussung der Funktionen, des Verhaltens oder des Betrieb des vernetzten Produkts), oder eine Wetter-App für Smart-TVs, die ihre Wetterdaten nicht vom Anbieter, sondern von anderen, offenen Datenquellen im Internet bezieht, die nicht als Erfüllungsgehilfen des Anbieters auftreten (keine bidirektionale Kommunikation mit dem Anbieter).

Ob das Produkt, mit dem der verbundene Dienst interagiert, vom Data Act in zeitlicher Hinsicht erfasst ist, spielt nach der hier vertretenen Ansicht wiederum keine Rolle. Ein Remote-Update-Service für ein Produkt, das nicht mehr verkauft wird, kann somit trotzdem ein verbundener Dienst sein und die vorvertraglichen Informationspflichten auslösen, selbst wenn für das gewartete Gerät keine Pflichten nach Data Act mehr bestehen.

In der Praxis kommen immer wieder unklare Fälle vor. Ein Beispiel wäre eine Predictive-Maintenance-Lösung für Landmaschinen: Wie ist ein Dienst zu beurteilen, der die von einem Traktor generierten Daten analysiert, um Wartungsintervalle vorherzusagen und den Betrieb des vernetzten Produkts zu optimieren? Ohne diesen Datenaustausch könnte die Funktion der vorausschauenden Wartung und der Optimierung des Betriebs nicht ausgeführt werden. Ist sie jedoch eine Funktion des vernetzten Produkts oder lediglich ein nachgelagerter Dienst, bei welchem anhand der Daten lediglich bestimmt wird, wann Teile ausgetauscht werden? Der Austausch führt nicht zu einer Anpassung der Funktion des Produkts, sondern erhält diese nur aufrecht. Wenn der Dienst aber basierend auf seiner Analyse zwecks Optimierung die Parameter der Landmaschinen justiert, dann läge in jedem Fall eine Einwirkung auf das Produkt und somit ein verbundener Dienst vor.

Die Legaldefinition bringt noch eine weitere Unklarheit mit sich. Sie lässt nämlich darauf schliessen, dass jede Software auf einem vernetzten Produkt ein verbundener Dienst ist. Ein solches Verständnis macht jedoch keinen Sinn, da fast jedes vernetzte Produkt in der einen oder anderen Form Software enthält (z.B. als Firmware in den Chips). Software kann daher vernünftigerweise nur dann ein verbundener Dienst sein, wenn sie nicht Teil des Produkts ist (wie z.B. das Betriebssystem der Smartwatch), sondern im Rahmen eines (separaten) Dienstes angeboten wird, auch wenn zum Dienst gehörende Software (z.B. eine App) auf dem vernetzten Produkt schon vorinstalliert ist. Nötig ist immerhin auch hier, dass sie mit dem Produkt interagiert, wie z.B. die Wetter-App auf dem Smart-TV die Wetterprognose im Internet abruft und sie auf dem TV anzeigt. Dieses Beispiel wäre allerdings auch eins, bei welchem möglicherweise gar keine Daten des Dienstes abrufbar sind und dessen Anbieter daher auch nicht als Dateninhaber gilt (zum Begriff des Dateninhabers sogleich); die Information nach Art. 3(3) würde entsprechend knapp ausfallen.

Kein verbundener Dienst läge auch dann vor, wenn ein Unternehmen eine Software für seine vernetzten Produkte separat lizenziert, mit welcher diese gesteuert oder sogar aufdatiert werden könnten, die Lieferung des Unternehmens aber darauf beschränkt ist, Software oder Updates für diese Software (nicht für das vernetzte Produkt) zu liefern, aber sonst keine Service-Komponente enthält, was das Produkt betrifft. Würde die Software hingegen in Kombination mit einem Update-Service für das vernetzte Produkt angeboten, läge bezüglich dieses Services ein verbundener Dienst vor, der über die Software zum Tragen kommt. Ebenfalls ein klassischer verbundener Dienst wäre natürlich der Fall, in welchem die Software in Form einer Dienstleistung (Software-as-a-Service) angeboten wird.

Das Pendant zu den Produktdaten beim vernetzten Produkt sind die sog. verbundenen Dienstdaten *(related service data)*. Gemeint sind hier gemäss Legaldefinition die 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. Es geht also vor allem um die Einträge von Logbüchern (z.B. wann ein Nutzer welche Funktion genutzt oder sich authentifiziert hat). Sie sind in der Praxis für Nutzer oft weniger interessant; genutzt werden solche Angaben vor allem von den Anbietern, um die Nutzung ihrer Produkte zu verstehen und diese zu verbessern.

Nicht erfasst sind analog zu den obenstehenden Ausführungen der Content, der im Rahmen eines Dienstes bearbeitet wird. Wird in einem Fahrzeug eine Musik-Strea-

17 Beispiele basierend auf Erwägungsgrund 17.

ming-App wie Spotify nachträglich installiert, ist sie ein verbundener Service (vom Anbieter der App, der folglich auch den Informationspflichten unterliegt). Die Musik selbst gilt nicht als Dienstdatum, die vom Nutzer erfasste Playlist ebenfalls nicht.[18] Die Angaben über die von ihm im Fahrzeug tatsächlich abgespielten Songs als digitalisierte Nutzerhandlungen wären hingegen konsequenterweise als Dienstdaten einzustufen –sofern sie abrufbar sind (diese letzte Voraussetzung ergibt sich zwar nicht aus der Legaldefinition, muss aber entsprechend dem Konzept des Data Act wie schon bei den Produktdaten so gelten).

Dasselbe müsste im Prinzip auch gelten, wenn die App auf einem Mobiltelefon (oder Notebook) installiert wird, weil ein solches Gerät letztlich ebenfalls ein vernetztes Produkt ist. Zwar sind Geräte, deren Hauptfunktion die Speicherung, Verarbeitung oder Übertragung von Daten gemäss der Ausnahme in der Legaldefinition in Art. 2 Ziff. 5 ist, keine vernetzten Produkte. Die Ausnahme gilt aber nur, wenn diese Funktionen für eine andere Partei als den Nutzer ausgeübt werden; beim Mobiltelefon erfolgt die Speicherung, Verarbeitung und Übertragung von Daten aber primär für den Nutzer selbst. Die anderen Kriterien der Legaldefinition für vernetzte Produkte erfüllen solche Geräte ohne Weiteres: Sie sammeln etwa Daten über die Umwelt (z.B. Standort, Helligkeit der Umgebung) und diese sind extern abrufbar. Es ist aber auch klar, dass der Gesetzgeber solche Geräte nicht im Sinn hatte; ein solches weites Verständnis des Anwendungsbereichs des Data Act führt im Prinzip dazu, dass die meisten Anbieter von Apps oder sonstiger Software, die eine wechselseitige Kommunikation des Anbieters mit dem Gerät ermöglicht (weil die App mit dem Server des Anbieters z.B. für Updates in Verbindung steht), erfasst sein dürften; das Kriterium, dass die Funktion, das Verhalten oder der Betrieb des Geräts in einer Form beeinflusst wird, wird eine solche Software fast immer erfüllen. Auch die Europäische Kommission geht in ihren FAQ zum Data Act davon aus, dass «die meisten, wenngleich nicht alle digitalen Dienste, die mit vernetzten Produkten interagieren» in die Kategorie der verbundenen Dienste fallen werden.[19] Dies heisst, dass alle Anbieter von solchen Apps die Pflichten gemäss Art. 3(1) und Art. 3(3) trifft. Ob die Nutzer identifiziert werden können oder nicht spielt dabei anders als im Datenschutz keine Rolle.

Ob ein derart breiter Anwendungsbereich tatsächlich beabsichtigt worden ist, darf zwar bezweifelt werden, aber es wäre nicht der erste Fall einer mangels durchdachter Legaldefinitionen überbreit angelegten Digital-Regulierung. Der EU AI Act ist ein weiteres solches Beispiel.[20]

VI. Dateninhaber

Wer an Produktdaten oder verbundene Dienstdaten gelangt, muss sich unter dem Data Act immer fragen, ob er allenfalls als Dateninhaber *(data holder)* gilt, was eine Reihe von Folgepflichten nach Art. 4 ff. nach sich zieht.

Auch hier ist die Legaldefinition nicht wirklich klar. In der deutschen Fassung gilt als Dateninhaber jede 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» (Art. 2 Ziff. 13). In der englischen Fassung ist es hingegen derjenige, der «im Einklang» *(in accordance with)* mit geltendem EU-Recht das Recht oder die Pflicht hat, Daten zu nutzen und bereitzustellen, und erfasst sind nicht nur Fälle, in denen eine Person im Rahmen eines verbundenen Dienstes an Daten gelangt.[21] Selbst die FAQ der Europäischen Kommission machen bisher einen weiten Bogen um die Definition des Dateninhabers; sie stellen nur klar, dass der Hersteller eines Geräts nicht automatisch auch Dateninhaber ist,[22] was selbstverständlich ist.

Nach dem Sinn und Zweck des Data Act muss die breitere Definition des englischen Wortlauts gelten. Es genügt demnach jeder *vertragliche* Zugang zu Daten, wobei damit im Ergebnis Produktdaten und verbundene Dienstdaten gemeint sind. Eine gesetzliche Pflicht oder ein gesetzliches Recht ist nicht nötig, weil sonst kaum jemand Dateninhaber wäre und Art. 4 ff. toter Buchstabe. Es sind wiederum Fälle denkbar, in denen eine Person auch ohne einen verbundenen Dienst zu erbringen zum Dateninhaber wird, z.B. wenn sie Wartungsdienste an Geräten vor Ort erbringt und für die Leistungserbringung Daten von den Geräten herunterladen und analysieren muss. Zwar könnte vertreten werden, dass sie dann eine vertragliche Pflicht zur Nutzung der Daten hat, nicht aber auch zu deren «Bereitstellung» (und somit ein notwendiges Kriterium nicht erfüllt wäre). Würde die Person in der Folge nicht als Dateninhaber gelten, könnte sie die erhobenen Daten unter dem Data Act frei verwenden. Dieses Verständnis steht aber nicht im Einklang mit dem letzten Halbsatz der englischen Legaldefinition, wonach es bei Anbietern von verbundenen Diensten genügt, dass sie an Daten gelangen und es nicht nötig ist, dass sie auch zu deren Bereitstellung berechtigt oder verpflichtet sein müssen.

Gemäss den FAQ der Kommission kommt als Dateninhaber allerdings nur in Frage, wer die vertragliche Pflicht oder das vertragliche Recht mit dem *Nutzer* hat.[23] Sie erwähnen das Beispiel eines Herstellers, der datengenerierende

18 Erwägungsgrund 16.
19 Europäische Kommission, FAQ (Fn. 4), Frage Nr. 10.
20 Dort ist der Begriff der künstlichen Intelligenz so breit definiert, dass sogar herkömmliche Kopierer mit Texterkennung als KI-Systeme gelten (D. Rosenthal, EU AI Act: Verordnung über künstliche Intelligenz, Jusletter 5. August 2024, Rz. 16).
21 Art. 2 Ziff. 13 im Worlaut: «'data holder' means a natural or legal person that has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation adopted in accordance with Union law, to use and make available data, including, where contractually agreed, product data or related service data which it has retrieved or generated during the provision of a related service».
22 Europäische Kommission, FAQ (Fn. 4), Frage Nr. 21.
23 Europäische Kommission, FAQ (Fn. 4), Frage Nr. 21, wobei die FAQ teils den Umstand einer vertraglichen Beziehung mit dem Nutzer mit

Komponenten von zwei Lieferanten verbaut, wovon nur der erste diese Daten direkt erhält und gegenüber dem Nutzer im Rahmen von Art. 3(2) offengelegt worden ist, während der zweite (nur) über den Hersteller an die Daten gelangt. Auf die Daten hat er gegenüber dem Hersteller zwar einen vertraglichen Anspruch, gilt nach den FAQ aber nicht als Dateninhaber. Der Hersteller muss allerdings vom Nutzer im Rahmen von Art. 4(13) das Recht erhalten haben, die Daten an Dritte – hier den zweiten Lieferanten des Herstellers – weiterzugeben. Diese Interpretation ist durch den Gesetzeswortlaut zwar nicht gestützt, erscheint aber sinnvoll, um den Kreis der Dateninhaber nicht ausufern zu lassen.

Zu weit geht die Kommission aber, wenn sie in diesem Zusammenhang behauptet, Art. 3(2) verlange die Offenlegung der Identität der Dateninhaber; das steht so nicht im Gesetz und macht auch keinen Sinn. Eine solche Pflicht sieht nur Art. 3(3) für den Fall eines verbundenen Dienstes vor.

Als Faustregel gilt somit, dass Dateninhaber jeder ist, der im Rahmen eines Vertrags mit dem Nutzer, etwa beim Erbringen eines verbundenen Dienstes, an Produktdaten oder verbundene Dienstdaten gelangt und diese nutzen darf oder muss. Davon kann es bei vernetzten Produkten und verbundenen Diensten mehrere geben. Der Gerätehersteller ist wiederum nicht per se Dateninhaber. Nicht erfasst sind nach heutigem Verständnis zudem, wie weiter vorne schon erwähnt, jene, die solche Daten lediglich im Auftrag eines anderen bearbeiten (also z.B. der Cloud-Provider eines Dateninhabers).[24]

VII. Herausgabepflichten des Dateninhabers

Der Grundsatz ist einfach und weitgehend: Wer Dateninhaber ist, muss auf Verlangen des Nutzers Produktdaten und verbundene Dienstdaten entweder dem Nutzer oder einem von ihm bezeichneten Dritten zur Verfügung stellen, einschliesslich der zur Auslegung und Nutzung der Daten erforderlichen Metadaten. Das muss er unverzüglich, einfach, sicher, in einem umfassenden, gängigen und maschinenlesbaren Format und – falls relevant und technisch durchführbar – in derselben Qualität wie für den Dateninhaber, kontinuierlich und in Echtzeit tun (Art. 4(1), Art. 5(1)). Den Nutzer darf das nichts kosten, vom Dritten kann der Dateninhaber hingegen ein Entgelt verlangen.

In der Praxis stellt sich vor allem die Frage, wie diese Herausgabe eingeschränkt werden kann oder sogar muss:

- Zunächst gilt die Pflicht nur für **Produktdaten** und **verbundene Dienstdaten**, was insofern relevant ist, als in der Praxis häufig auch veredelte Daten anfallen. Die Pflicht gilt zudem nur für Daten, die für den Dateninhaber «ohne Weiteres» verfügbar *(readily available)* sind (Art. 4(1), Art. 5(1)). Er muss also wegen des Data Acts keine neue Programmierung oder dergleichen vornehmen, um an die Daten heranzukommen, um bestimmte Daten zu extrahieren, die er nicht schon selbst hat. Er muss auch sonst keinen unverhältnismässigen Aufwand zur Beschaffung der Daten betreiben (Art. 2 Ziff. 17), wogegen der Aufwand für deren Bereitstellung nicht zählt. Sind Daten zwar vorhanden, aber nicht dem Nutzer zugeordnet, so gelten sie dennoch als ohne Weiteres verfügbar, wenn angemessene Mittel bestehen, um sie erneut einem spezifischen Nutzer oder Produkt zuzuordnen.[25] Eine Pflicht, Daten aufzubewahren, weil ein Nutzer sie nachfragen könnte, gibt es hingegen nicht.
- All jene Daten, auf die der **Nutzer selbst schon zugreifen** könnte (insbesondere gestützt auf Art. 3(1)), müssen diesem nicht nochmals geliefert werden, auch wenn das für den Nutzer viel bequemer sein mag (Art. 4(1)); diese Ausnahme gilt jedoch nicht, wenn es um die Herausgabe an Dritte geht (Art. 5).
- Die Herausgabe von **Geschäftsgeheimnissen** des Dateninhabers (oder eines dritten Geheimnisherrn) kann davon abhängig gemacht werden, dass es Massnahmen zu deren Schutz gibt. Nahe liegen Geheimhaltungspflichten und Nutzungsbeschränkungen, aber denkbar wären auch technische Massnahmen (wie z.B. asymmetrische Verschlüsselungen, die einen Zugriff nur durch den Nutzer oder den Dritten erlauben). Was als Geschäftsgeheimnis gelten kann, ergibt sich aus der EU-Geschäftsgeheimnisrichtlinie[26] bzw. den nationalen Umsetzungsgesetzen. Was konkret als Geschäftsgeheimnis gilt, bestimmt der Geheimnisherr und muss als solches deklariert werden (praktischerweise vom Dateninhaber, der mit dem Geheimnisherr nicht identisch sein mag), spätestens sobald ein Antrag auf Herausgabe vorliegt.[27] Die Schutzmassnahmen sind zu vereinbaren zwischen dem Dateninhaber und dem Nutzer bzw. dem Dritten. Gelingt dies nicht oder werden sie nicht befolgt, kann die Herausgabe ausgesetzt oder verweigert werden (Art. 4(7), Art. 5(10)). Weist der Dateninhaber nach, dass er bzw. der Geheimnisherr trotz Massnahmen «mit hoher Wahrscheinlichkeit … schweren wirtschaftlichen Schaden durch die Offenlegung von Geschäftsgeheimnissen erleiden wird», dann kann er die Herausgabe ebenfalls ablehnen (Art. 4(8), Art. 5(11)). Zu diesen Fällen der sog. *Trade Secret Handbrake* dürfte es aber selten kommen, da der Data Act vorsieht, dass in solchen Fällen immer auch die zuständige

dem Umstand einer Identifikation des Dateninhabers gegenüber dem Nutzer vermischen.

24 Erwägungsgrund 22.

25 Europäische Kommission, FAQ (Fn. 4), Frage Nr. 13a.

26 Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung (‹eur-lex.europa.eu/eli/dir/2016/943/oj›, zuletzt abgerufen am 29. Oktober 2025); Nach Art. 2 Ziff. 1 der Richtlinie gelten als Geschäftsgeheimnisse alle Information, die alle nachstehenden Kriterien erfüllen: a) Sie sind in dem Sinne geheim, dass sie weder in ihrer Gesamtheit noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne weiteres zugänglich sind; b) sie sind von kommerziellem Wert, weil sie geheim sind; c) sie sind Gegenstand von den Umständen entsprechenden angemessenen Geheimhaltungsmassnahmen durch die Person, die die rechtmässige Kontrolle über die Informationen besitzt.

27 Europäische Kommission, FAQ (Fn. 4), Frage Nr. 23.

Aufsichtsbehörde informiert werden muss, was eine faktische Hürde darstellt. Der Nutzer bzw. der Dritte kann die Herausgabe auch gerichtlich durchzusetzen versuchen (Art. 4(9), Art. 5(12)).

- Unabhängig von dieser Trade Secret Handbrake gewährt im Falle der Herausgabe an einen Dritten Art. 5(9) noch eine weitere, indirekte Einschränkungsmöglichkeit: Demnach müssen Geschäftsgeheimnisse Dritten gegenüber nur insoweit offengelegt werden, als diese Offenlegung **für den zwischen dem Nutzer und dem Dritten vereinbarten Zweck unbedingt erforderlich** ist. Aus diesem Grund sollte der Dateninhaber vom Nutzer verlangen, über diesen Zweck ins Bild gesetzt zu werden. Was die beiden festgelegt haben, entzieht sich freilich der Kontrolle des Dateninhabers und kann von Letzterem grundsätzlich auch nicht eingeschränkt werden.
- Dieses Regime zum Schutz von Geschäftsgeheimnissen gilt wie erwähnt nicht für den Zugang, der dem Nutzer **im Rahmen von Art. 3(1)** zu gewähren ist. Der Data Act verbietet nach der hier vertretenen Ansicht aber nicht, dass der Zugang nach Art. 3(1) für den Nutzer von der Vereinbarung vergleichbarer Schutzmassnahmen abhängig gemacht wird (z.B. vertragliche Geheimhaltungspflichten).[28] Dies ist somit Verhandlungssache. Wir empfehlen daher, bereits im Vertrag über den Verkauf eines vernetzten Produkts oder im Vertrag über einen verbundenen Dienst passende Geheimhaltungspflichten und Verwendungsbeschränkungen vorzusehen, wo es Geschäftsgeheimnisse gibt.
- Auch **Sicherheitsgründe** – zum Schutz von Maschinen und Menschen – können die Einschränkung oder Verweigerung der Herausgabe begründen, sofern das EU-Recht die entsprechende Sicherheit verlangt (z.B. bei Produkten im Rahmen des Cyber Resilience Act) (Art. 4(2); eine parallele Norm bei der Herausgabe an Dritte ging vermutlich vergessen). Auch hier ist der Einbezug der zuständigen Behörde nötig.
- Ein besonderes Augenmerk gilt etwaigen **Personendaten**, die natürlich auch in Produktedaten und verbundenen Dienstdaten enthalten sein können. Das spielt dann eine Rolle, wenn der Nutzer nicht die betroffene Person ist. Ein typischer Fall ist der Arbeitgeber, der ein System benutzt, das die Benutzung durch die Mitarbeitenden zuordnungsbar protokolliert. In diesen Fällen muss der Nutzer, der die Herausgabe verlangt, den Nachweis erbringen, dass er zum Erhalt und weiteren Bearbeitung dieser Daten nach DSGVO berechtigt ist, also namentlich über einen Rechtsgrund nach Art. 6 DSGVO verfügt (z.B. Einwilligung der Personen oder berechtigtes Interesse) und ggf. die Bedingungen von Art. 9 DSGVO erfüllt sind (Art. 4(12)). Das gilt auch dann, wenn der Dateninhaber die betroffenen Personen selbst nicht identifizieren kann; es zählt unseres Erachtens die Identifizierbarkeit seitens des Empfängers. Für die Herausgabe an Dritte gilt dasselbe Prinzip, wobei der Nutzer wie auch der Dritte diesen Nachweis erbringen kann (Art. 5(7)). Welche Anforderungen an diesen Nachweis zu stellen sind, definiert der Data Act allerdings nicht; in der Praxis dürfte es genügen, wenn eine solche Rechtsgrundlage glaubhaft ist, sie kann aber zur Absicherung des Dateninhabers mit einer Schadloshaltung verknüpft werden. Ist unklar, ob eine Rechtsgrundlage besteht, wird dem Dateninhaber das Recht zugestanden, die Daten vorab zu anonymisieren,[29] doch ist er nach unserer Ansicht dazu nicht verpflichtet. Er kann in solchen Fällen die Herausgabe von Personendaten bis zum Nachweis der Berechtigung schlicht verweigern. Ihn trifft übrigens auch die Verantwortung, nur jene Personendaten zu liefern, die durch die betreffende Rechtsgrundlage gedeckt sind.[30] Dies kann in der Praxis durchaus herausfordernd sein, etwa wenn ein Produkt von mehreren natürlichen Personen als Nutzer genutzt wird, z.B. ein Mietwagen. In solchen Fällen müsste zeitlich abgegrenzt werden, wer das Fahrzeug zu welcher Zeit genutzt hat, damit einem aktuellen Mieter nicht Daten herausgegeben werden, die einen Vormieter betreffen. Allerdings gilt auch hier: Was sich an Daten auf dem Produkt selbst abrufen lässt (d.h. via Art. 3(1)), unterliegt dieser Einschränkung des Data Act nicht. Hier muss nach den datenschutzrechtlichen Grundsätzen beurteilt werden, ob z.B. der Anbieter eines verbundenen Diensts als «Controller» gilt, der in diesem Fall Personendaten bekanntgibt, oder ob dies in der Verantwortung des Nutzers liegt.
- Geht es um die Herausgabe von Daten an Dritte, so kann sich die Frage stellen, ob der Dateninhaber diese verweigern kann, wenn es Anzeichen dafür gibt, dass er diese entgegen der **Absprache des Dritten mit dem Nutzer** verwendet oder sie z.B. nicht nach Gebrauch löscht; Art. 6(1) sieht nämlich vor, dass der Dritte sich an solche Einschränkungen zu halten hat. Die Frage lässt sich nicht klar beantworten; ein ausdrückliches Verweigerungsrecht sieht Art. 5 zwar nicht vor (wie etwa beim Schutz von Geschäftsgeheimnissen; dieser Umstand spricht gegen ein Recht zur Verweigerung). Die Pflicht zur Herausgabe nach Art. 5 existiert allerdings nicht in einem Vakuum, sondern unter der Annahme, dass (auch) Art. 6 befolgt wird. Zudem sieht Art. 11(1) vor, dass ein Dateninhaber geeignete Massnahmen vorsehen kann, um die Einhaltung (auch) von Art. 6 sicherzustellen. Art. 11(2) sieht sogar Löschansprüche bei zweckwidriger Nutzung vor. Angesichts dessen muss es dem Dateninhaber auch erlaubt sein, seine Daten gar nicht erst herauszugeben, wenn von einem solchen Verstoss ausgegangen werden muss, oder den Dritten zur Einhaltung der Zweckbindung direkt zu verpflichten (auch wenn die Nutzungsbeschränkung nach Art. 6(1) nur zwischen dem Nutzer und dem Dritten vereinbart wird). In der Praxis kann es sich jedenfalls lohnen, diesen Aspekt in einem Vertrag mit dem Nutzer und dem Dritten zu regeln. Dies ist von praktischer Relevanz, weil es sich bei diesen Dritten oft um Mitbewerber des Dateninhabers handeln wird und wenig Interesse besteht,

28 So auch Europäische Kommission, FAQ (Fn. 4), Frage Nr. 24.
29 Europäische Kommission, FAQ (Fn. 4), Frage Nr. 25a.
30 Europäische Kommission, FAQ (Fn. 4), Frage Nr. 25b.

diese bei der Bearbeitung des eigenen Kunden zu unterstützen.

- Eine Herausgabe an einen **Dritten mit Sitz ausserhalb der EU** ist unter dem Data Act nicht erforderlich, auch wenn ein Nutzer dies verlangt (Art. 3(3) lit. d);[31] der die Herausgabe verlangende Nutzer muss im Übrigen ebenfalls in der EU sein.[32]
- In der Praxis kann auch die Frage der **Identifizierung des Nutzers** und der Umgang mit **wechselnden Nutzern** Herausforderungen mit sich bringen. Eine Herausgabepflicht besteht nur gegenüber der natürlichen oder juristischen 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» (Art. 2 Ziff. 12). Erfolgt eine Anfrage betreffend ein Produkt, kann vom Nutzer verlangt werden, dass er sein Eigentum bzw. Besitz (was gemeint ist, ist nicht klar) oder seinen vertraglichen Nutzungsanspruch ausweist, einschliesslich des Umstands, dass dieser noch besteht. Bei einem verbundenen Dienst ist der Nachweis in der Regel einfacher, weil der Leistungsempfänger normalerweise vom Dateninhaber über eine Benutzerkennung identifiziert werden kann. Solches kann auch bei vernetzten Produkten vorgesehen werden, etwa indem dem Erwerber (als Hauptnutzer) und den weiteren, von ihm vertraglich ermächtigten Personen (als weitere Nutzer) die Möglichkeit gegeben wird, sich als «Nutzer» zu registrieren. Nicht jede Nutzung führt jedoch auch zur Stellung eines Nutzers im Sinne des Data Act. Das gilt auch bei der Nutzung fremder «Produkte»: Wer mit seinem Fahrzeug eine intelligente Strasse befährt und in der Folge von dieser Sensorwerte empfängt, wird deswegen noch nicht zu deren Nutzer im Sinne des Data Acts.[33]
- In **zeitlicher Hinsicht** hat ein Nutzer jeweils Anspruch auf alle zum Zeitpunkt seiner Anfrage vorhandenen Produktdaten bzw. verbundenen Dienstdaten, also auch auf jene Daten, die vor seiner Zeit als Nutzer angefallen sind (sie können z.B. relevant sein, um die Wartungshistorie eines Produkts zu beurteilen).[34] Vorbehalten bleiben darin allenfalls enthaltene Personendaten früherer Nutzer; deren Rechte gehen vor. In Bezug auf Geschäftsgeheimnisse früherer Nutzer können die Regeln zu deren Schutz nach Art. 4 und Art. 5 angewendet werden, sofern diese Nutzer die Daten als Geschäftsgeheimnisse deklariert hatten (dieser Schutz steht nicht nur dem Dateninhaber, sondern auch anderen Geheimnisherrn zu, allerdings wird dies mit dem Dateninhaber so vereinbart sein müssen).
- Eine **Herausgabe von Daten an einen Torwächter** *(gatekeeper)* gemäss Digital Markets Act (DMA)[35] ist ebenfalls nicht vorgesehen (Art. 5(3)). Die Google-Mutter Alphabet gilt zum Beispiel unter anderem in Bezug auf Google Maps, die Google Suche und Youtube als solcher Torwächter, Meta beispielsweise in Bezug auf Facebook und WhatsApp, Microsoft in Bezug auf LinkedIn.[36] Der Grund dahinter ist, dass sie ihre bereits bestehende Machtposition nicht noch durch Daten ihrer Nutzer ausbauen können sollen. In der Praxis ist die Umsetzung dieser Vorgabe nicht ganz trivial, da nicht ohne Weiteres klar ist, welche einzelnen juristischen Personen zum Kreis der betroffenen Torwächter gehören.

Der Data Act sieht noch weitere Einschränkungen für Nutzer vor. Dazu gehört etwa das Verbot, dass sich Nutzer in die Systeme des Dateninhabers «hacken» dürfen, um Zugang zu erhalten (Art. 4(11)), und die Daten auch nicht benutzen dürfen, um konkurrierende vernetzte Produkte zu entwickeln, oder um Einblicke in die wirtschaftliche Lage oder etwa die Produktionsmethoden des Herstellers oder Dateninhabers zu erhalten (Art. 4(13)). Diese Vorgaben gelten auch für Dritte, die auf Wunsch der Nutzers Daten erhalten (Art. 5(6)); sie dürfen die Daten auch nicht in einer Weise verwenden, welche die Sicherheit des vernetzten Produkts oder verbundenen Dienstes schwächt (Art. 6(2) lit. f)

Die Herausgabepflichten des Data Act stehen im Übrigen in Konkurrenz zu den Rechten von betroffenen Personen nach DSGVO, insbesondere das Recht auf Auskunft (Art. 15 DSGVO) und Datenportabilität (Art. 20 DSGVO). Art. 1(5) stellt klar, dass die DSGVO durch den Data Act in keiner Weise eingeschränkt wird. Ist der Nutzer also zugleich betroffene Person, kann ihm die Auskunft bzw. Herausgabe seiner Personendaten nicht gestützt auf den Data Act eingeschränkt werden.

VIII. Nutzungsbeschränkungen des Dateninhabers

In der Praxis mitunter noch wichtiger als die Herausgabepflichten des Dateninhabers wird für viele Unternehmen die Regelung von Art. 4(13) sein, wonach ein Dateninhaber die ihm zugänglichen Produktdaten und verbundenen Dienstdaten nur dann für eigene Zwecke verwenden darf, wenn er sich darüber mit dem Nutzer geeinigt hat.

Teilweise wird vertreten, auch die Nutzung für die Zwecke des Nutzers bzw. für die Erbringung eines verbundenen Dienstes sei von dieser Bestimmung erfasst bzw. unterliege ihr. Unternehmen benutzen dieses Argument, um Nutzer zum Abschluss einer Vereinbarung zu drängen, die ihnen dann aber vor allem auch die Eigennutzung der Daten erlaubt. Denn darum ging es dem Gesetzgeber: Er hatte Verwendungszwecke wie die Verbesserung der Funktionsweise des vernetzten Produkts oder verbundener Dienste im Sinn, die Entwicklung neuer Produkte oder Dienste oder die Ag-

31 Die Pflicht zur Information über die Möglichkeit der Datenweitergabe an Dritte nach Art. 3(3) lit. d bezieht sich nur auf in der Union niedergelassene Dritte. Obwohl Art. 5, der die eigentliche Herausgabepflicht regelt, diese territoriale Einschränkung nicht explizit wiederholt, wird allgemein davon ausgegangen, dass keine Pflicht zur Herausgabe an Dritte ausserhalb der EU besteht.

32 Europäische Kommission, FAQ (Fn. 4), Frage Nr. 37.

33 Europäische Kommission, FAQ (Fn. 4), Frage Nr. 7.

34 Europäische Kommission, FAQ (Fn. 4), Frage Nr. 32.

35 Verordnung (EU) 2022/1925.

36 Vgl. die Bekanntmachung der initialen Benennung vom 6. September 2023 durch die Europäische Kommission (‹ec.europa.eu/commission/presscorner/detail/de/ip_23_4328›, zuletzt abgerufen am 29. Oktober 2025).

gregation von Daten mit dem Ziel, die Erkenntnisse Dritten zu verkaufen.[37] Die Nutzung der Daten zwecks Erbringung der Leistung an den Nutzer ist bereits implizit durch die Vereinbarung der Leistungserbringung vereinbart und bedarf daher keiner ausdrücklichen Nennung, um rechtmässig zu sein; alles andere wäre absurd.

Die Anforderungen an die vertragliche Grundlage der Eigennutzung der Daten sind jedenfalls gestützt auf die Erwägungen nicht sehr hoch. Jede Vertragsklausel, nach der der Dateninhaber die Produktdaten oder verbundenen Dienstdaten nutzen darf, sollte für den Nutzer transparent sein, auch in Bezug auf die Zwecke, zu denen der Dateninhaber die Daten zu verwenden beabsichtigt, heisst es in Erwägungsgrund 25.

Es sind jedoch einige Punkte in der Praxis zu berücksichtigen:

- Zunächst gilt die Einschränkung von Art. 4(13) nur für (ohne Weiteres verfügbare) Produktdaten und verbundene Dienstdaten, und auch hier unter **Ausschluss von Personendaten**. Dies bedeutet im Umkehrschluss, dass es für die Nutzung von anderen Daten (namentlich **veredelte Daten**) oder Personendaten keine solche Regelung braucht.
- In **zeitlicher Hinsicht** gilt Art. 4(13) zunächst für seit dem 12. September 2025[38] angefallene Daten. Das gilt grundsätzlich auch für Daten von Produkten, die vor dem 12. September 2025 in Verkehr gebracht worden sind. Es muss also auch mit den bestehenden Nutzern eine vertragliche Grundlage geschaffen werden. Die Kommission vertritt in ihren FAQ allerdings die Ansicht, dass wenn ein Nutzer nicht bekannt ist, die Bearbeitung seiner Daten zwar fortgesetzt werden kann, bei Bekanntwerden des Nutzers jedoch eine Vereinbarung mit ihm zu treffen ist.[39]
- Der Dateninhaber unterliegt nach Art. 4(14) der zusätzlichen Einschränkung, dass Produktdaten (verbundene Dienstdaten werden nicht erwähnt) nur dann **an Dritte weitergegeben** werden dürfen, wenn dies der Erfüllung des Vertrags mit dem Nutzer dient. Will der Dateninhaber das zu eigenen Zwecken tun, ist dies im Vertrag mit dem Nutzer entsprechend klar festzuhalten. Unklar ist, ob die Weitergabe als eigentliche Pflicht des Dateninhabers formuliert sein muss; nach der hier vertretenen Ansicht ist dem nicht so; es muss dem Nutzer freistehen, dem Dateninhaber die Weitergabe auch bloss zu erlauben, sind es doch seine Daten. Ist dem Dateninhaber die Weitergabe an einen Dritten nur zu einem bestimmten Zweck erlaubt, muss er den Dritten entsprechend verpflichten.
- Art. 4(13) sieht als **Einschränkung** vor, dass der Dateninhaber die Daten einerseits nicht verwenden darf, um Einblicke in die wirtschaftliche Lage, Vermögenswerte und Produktionsmethoden des Nutzers zu gewinnen, anderseits aber auch die wirtschaftliche Nutzung der Daten durch den Nutzer selbst nicht untergraben darf. Letzteres kann dahingehend interpretiert werden, dass die vertragliche Regelung der Eigennutzung der Daten durch den Dateninhaber erstens nicht exklusiver Natur sein darf und zweitens mindestens kündbar sein muss, weil es für den Nutzer möglich bleiben soll eine andere Nutzung seiner Daten vorzusehen (etwa weil jemand dafür bezahlt, die Daten exklusiv zweitverwerten zu können, d.h. nicht will, dass der Dateninhaber sie weiterhin auch für sich nutzt). Dem kann allerdings entgegenhalten werden, dass diese Einschränkungen nur soweit gelten, als sie den Nutzer auf seinen eigenen Märkten in relevanter Weise tangieren, was nicht oft der Fall sein wird.
- Zu beachten ist ferner, dass **Geheimhaltungsklauseln** in vielen Verträgen erfahrungsgemäss bereits eine Boilerplate-Regelung enthalten, wonach Daten der Parteien nicht für vertragsfremde Zwecke verwendet werden dürfen. In solchen Fällen ist es wichtig, die vorstehende erwähnte Nutzungsbefugnis einer solchen Regelung der Geheimhaltungsklausel vorgehen zu lassen. Wir empfehlen zudem, eine vertragliche Nutzungsbefugnis über den Anwendungsbereich von Art. 4(13) hinaus zu formulieren (also z.B. auch die Eigennutzung von anderen Datenkategorien und von Personendaten vorzusehen, obwohl Art. 4(13) dies selbst nicht verlangen würde), da sonst Befugnislücken entstehen können oder Streit darüber entsteht, wofür der Dateninhaber die Daten seines Kunden verwenden darf.

Die in der Praxis gewichtigste Herausforderung ist in diesem Zusammenhang allerdings der Umstand, dass die vertragliche Regelung bzw. Zustimmung zur Eigennutzung durch den Dateninhaber immer mit jedem jeweiligen Nutzer getroffen sein muss. Denn dieser Nutzer kann ändern (Weiterverkauf, Weitervermietung), und es können mehrere Nutzer zugleich bestehen (z.B. Leasinggesellschaft und Leasingnehmer, Eigentümer und Mieter). Je nach Verständnis des Begriffs des Dateninhabers hat dieser mit dem Nutzer möglicherweise gar keinen Vertrag. So oder so muss sichergestellt werden, dass in jedem Vertrag mit jedem Nutzer eine Regelung über die Eigennutzung der anfallenden Daten inklusive Weitergabe an Dritte vorgesehen ist, was bei entsprechenden Vertriebsstrukturen eine Herausforderung sein kann. Wer sich in seinen AGB ein entsprechendes Recht einräumen lässt, muss also den Erwerber verpflichten, dieses Recht an einen nachgelagerten Käufer zu überbinden.

IX. Vertragliche Vereinbarungen

In der Praxis zeichnet sich ab, dass nicht nur die Regelungen zur Eigennutzung von Daten zwischen den Stakeholdern im Markt vertraglich festgehalten werden, sondern auch die Herausgabe von Daten und deren Modalitäten wie etwa die Identifikation des Nutzers oder die Art und Weise, wie Anfragen zu stellen sind. Eine von der Europäischen Kommission eingesetzte Expertengruppe hat z.B. im April 2025 zu diesem Zweck für den B2B-Bereich ihre Vorschläge für verschiedene «Model Contract Terms» publiziert.[40] Sie sollen

37 Erwägungsgrund 25.
38 Art. 50.
39 Europäische Kommission, FAQ (Fn. 4), Frage Nr. 34a.
40 Der Bericht der Expert Group on B2B data sharing and cloud computing contracts ist abrufbar unter ‹ec.europa.eu/transparency/expertgroups-register/core/api/front/document/116180/download›, zuletzt abgerufen am 29. Oktober 2025; Link zur Sitzung: ‹ec.europa.eu/trans

als Vorlage für Modellverträge dienen, die die Europäische Kommission publizieren muss. Die uns bisher bekannten Modellverträge sind für den praktischen Einsatz jedoch leider nur beschränkt tauglich und lückenhaft. Sie ernteten bereits Kritik aus Datenschutzkreisen.[41]

Die vertragliche Regelung der Umsetzung des Data Act bringt auch taktische Fragen mit sich. So kann ein Nutzer abgesehen vom Sonderfall von Geschäftsgeheimnissen an sich nicht gezwungen werden, sich auf einen Vertrag mit dem Dateninhaber einzulassen, der Letzterem weitere Rechte einräumt oder die Herausgabe von Daten regelt – seine Rechte stehen dem Nutzer von Gesetzes wegen zu. Jede Klausel, die die Rechte des Nutzers gemäss den erwähnten Bestimmungen des Data Acts zu dessen Nachteil ausschliesst, davon abweicht oder die Wirkung dieser Rechte abändert, ist für den Nutzer ohnehin unwirksam (Art. 7(2)).

In der Praxis sehen wir drei Vorgehensweisen:

- In den Verträgen über den Verkauf von vernetzten Produkten und verbundenen Diensten wird festgehalten, wo die vorvertraglichen Informationen abzurufen sind, wie der Hersteller (als Dateninhaber oder auch sonst) die Daten des Nutzers auch sonst verwenden (und weitergeben) darf und dass diese Klausel an nachgelagerte Erwerber und andere Nutzer zu überbinden ist. Eine solche Klausel wird in der Regel in die AGB aufgenommen.
- n den Verträgen über den Verkauf von vernetzten Produkten und verbundenen Diensten wird zusätzlich auch der Prozess zur Herausgabe von Daten an den Nutzer und an Dritte festgehalten, inklusive dem Verfahren zur Einreichung einer Anfrage, dem Umgang mit Personendaten und Berufsgeheimnissen sowie weitere Modalitäten. Die frühe Einbindung (z.B. als Ergänzung der bestehenden AGB) kann es einfacher machen, die Klauseln gegenüber dem Nutzer durchzusetzen.
- Die Herausgabe wird erst im Falle einer konkreten Anfrage für eine solche geregelt.

Rechtlich erforderlich ist eine vertragliche Regelung der Herausgabe mit dem Nutzer aber trotz allem grundsätzlich nicht, da sie gesetzlich geregelt ist. Wenn Unternehmen also behaupten, der Data Act erfordere zwingend eine Anpassung der Verträge, damit verbundene Dienste nach dem 12. September 2025 weiterhin erbracht werden können,[42] so trifft dies nicht zu. Erforderlich ist die Vertragsanpassung in solchen Fällen typischerweise «nur» zum Zweck, dem Anbieter die Eigennutzung zu erlauben, wo dies bisher nicht schon der Fall war.

Anders verhält es sich im Verhältnis zwischen Dateninhabern und Dritten, denen diese Daten nach Art. 5 zur Verfügung gestellt werden müssen. Hier ist ein Vertrag erforderlich, da für die Bereitstellung von Daten hier vom Dritten (nicht dem Nutzer) auch ein Entgelt verlangt werden darf. Rechtlich gelten dafür einerseits die Bestimmungen von Art. 5 und 6, die die Pflicht zur Herausgabe an die Dritten regeln (und in Bezug auf die Daten für diese Dritten geltenden Einschränkungen), und die Art. 8–13, welche den Vertrag regeln.

In den meisten Fällen wird auch zwischen dem Nutzer und Dritten ein Vertrag bestehen, der üblicherweise der Grund dafür ist, dass der Nutzer den Dateninhaber überhaupt anweist, dem Dritten seine Daten zugänglich zu machen. Typisches Beispiel ist der Fall, in welchem ein Nutzer sein vernetztes Produkt neu nicht mehr vom Hersteller warten lassen will, sondern von einem anderen Anbieter. Diesem soll der Hersteller (als bisheriger Dateninhaber) nun die dafür nötigen Daten zugänglich machen. Es sind aber auch völlig andere Beispiele denkbar, wie z.B. die Weitergabe von Fahrzeugdaten an eine Versicherung, die dem Nutzer eine Prämienreduktion verspricht, solange dieser gestützt auf die Fahrzeugdaten risikoarm fährt (dies ist auch ein Beispiel, in welchem der Nutzer ein Interesse an einer direkten Übermittlung der Daten an den Dritten durch den Dateninhaber hat – sie garantiert, dass die Daten nicht manipuliert sind).

Die Art. 8–13 regeln Verträge über die Lieferung von Daten von einem Unternehmen an ein anderes ganz generell, und zwar immer dann, wenn das Recht der EU oder eines der Mitgliedsstaaten eine Pflicht zur Datenbereitstellung vorsieht. Sie finden also auch für die Fälle gemäss Art. 5 Anwendung, aber nicht nur. Es gelten dabei folgende Grundsätze:

- Die Datenlieferung muss zu fairen, angemessen und nichtdiskriminierenden Bedingungen erfolgen (Art. 8(1)). Dieses sog. **FRAND-Prinzip**[43] gilt z.B. auch im Patentrecht, wo es um die Lizenzierung wesentlicher Technologien geht. Es bedeutet unter anderem, dass alle Dritten, denen Daten geliefert werden müssen, gleich zu behandeln sind. Das ist dort von spezieller Bedeutung, wo ein Dateninhaber Daten eines Nutzers bereits seinen eigenen Konzerngesellschaften zur Verfügung stellt; die Konkurrenz muss er – nach Massgabe ihrer Gleichheit – gleich behandeln (Art. 8(3)).
- Für Datenlieferungen kann vom Dritten ein **Entgelt** verlangt werden, das nebst Selbstkosten und Investitionsbeiträgen auch eine Marge enthalten darf, Letzteres ausgenommen bei KMU und Non-Profit-Forschungseinrichtungen (Art. 9). Es ist wiederum auf Gleichbehandlung

parency/expert-groups-register/screen/meetings/consult?lang=en&meetingId=61683&fromExpertGroups=3840›, zuletzt abgerufen am 29. Oktober 2025.

41 European Data Protection Board, Statement 4/2025 on the European Commissions Recommendation on draft non-binding model contractual terms on data sharing under the Data Act, vom 8. Juli 2025, abrufbar unter ‹www.edpb.europa.eu/system/files/2025-07/edpb_statement_202504_commission-s_draftmcts_dataact_en.pdf›, zuletzt abgerufen am 29. Oktober 2025.

42 Beispiel einer solchen Formulierung: «According to the EU Data Act, as a manufacturer of connected products and services, we are obliged to create a legal basis (End User License Agreement) with you as a user of these services. The EU Data Act will come into force on September 12, 2025. In order for [redacted] to continue providing you with digital services and other data-based products and services, we are obliged by the EU Data Act to conclude an additional contract that enables the processing of vehicle data necessary for delivering these services. You will receive this contract via [redacted] and via the [redacted] sales organization».

43 Steht für «Fair, Reasonable and Non-Discriminatory».

zu achten, insbesondere im Verhältnis konzerninterner Datenlieferungen und solche an externe Dritte. Eine fortgeschrittene, wenn auch rechtlich noch nicht gefestigte Überlegung ist, einen Teil der Forschungs- und Entwicklungskosten (F&E) der vernetzten Produkte in die Berechnung des Entgelts nach Art. 9 einzubeziehen. Es könnte argumentiert werden, dass F&E-Investitionen eine Voraussetzung für die «Sammlung und Erzeugung von Daten» sind und ihre Berücksichtigung die Anreize für Innovationen wahrt, wie es die Erwägungsgründe 30 und 46 des Data Acts vorsehen. Dies könnte als Mittel dazu dienen, die Hürden für Datenanfragen von Wettbewerbern zu erhöhen.

- Es können im Vertrag durchaus auch **Massnahmen zum Schutz** der Einhaltung von Art. 4, 5, 6, 8 und 9 vereinbart werden (z.B. Nutzungsbeschränkungen durch den Dritten).
- Es müssen die Vorgaben von Art. 13 eingehalten werden. Art. 13 definiert eine Reihe von **Vertragsregelungen, die als missbräuchlich gelten** und diesfalls unwirksam sind, falls sie einer Vertragspartei einseitig auferlegt worden sind. Das soll vor allem KMU schützen. Als missbräuchlich gelten Regelungen, welche von der guten Geschäftspraxis beim Datenzugang und bei der Datennutzung grob abweichen, insbesondere indem sie die Haftung für Vorsatz oder grobe Fahrlässigkeit ausschliessen, Rechtsbehelfe bei Nichterfüllung ausschliessen oder einer Partei das alleinige Recht zur Konformitätsbestimmung oder Vertragsauslegung einräumen, wobei zudem eine Missbräuchlichkeit vermutet wird, wenn sie unter anderem Rechtsbehelfe oder Haftung unangemessen beschränken, den Zugriff auf Daten zum erheblichen Nachteil der anderen Partei ermöglichen, die Nutzung eigener Daten verhindern, eine Kündigung innerhalb einer angemessenen Frist verhindern, die Aushändigung einer Datenkopie verhindern, eine Kündigung mit unangemessen kurzer Frist ermöglichen oder wesentliche Vertragsänderungen ohne triftigen Grund und Kündigungsrecht erlauben (Art. 13(3)–(5)). Diese Regeln gelten für Verträge, die nach dem 12. September 2025 geschlossen wurden; für ältere Verträge ab dem 12. September 2027, falls diese auf unbeschränkte Dauer oder für zehn Jahre oder länger abgeschlossen wurden (Art. 50).

In diesem Bereich des Data Act wird anerkannten Modellverträgen voraussichtlich eine grössere Bedeutung zukommen, da sie entsprechende Rechtssicherheit bieten: Sie dürften per se der «guten Geschäftspraxis» entsprechen und daher nicht missbräuchlich sein (vgl. Art. 13(3)). Die Europäische Kommission erarbeitet derzeit solche Modellverträge für verschiedene Konstellationen unter dem Data Act bzw. wird sie zum Zeitpunkt des Erscheinens dieses Beitrags möglicherweise schon publiziert haben; sie bleiben allerdings freiwillig.

Art. 13 dürfte über die Weitergabe von Daten nach Art. 4 ff. hinaus von praktischer Relevanz sein, da sie grundsätzlich bei jedem B2B-Vertrag zu beachten sind, welcher (auch) den Zugang zu und die Nutzung von Daten oder die Verantwortlichkeit bei der Verletzung von datenrechtlichen Bestimmungen regelt (Art. 13(1)). Das kann Verträge im Bereich des Cloud-Computing ebenso betreffen wie den Kreditvertrag mit einer Bank, welcher ein Data-Sharing vorsieht.[44] Es darf gespannt beobachtet werden, ob Art. 13 überhaupt zur Kenntnis genommen werden wird.

X. Empfehlungen zur praktischen Umsetzung

Die praktische Umsetzung der Vorgaben des Data Acts (im hier diskutierten Bereich) kann in drei Schritten koordiniert werden.

In einem ersten Schritt ist der Anwendungsbereich zu klären und ein Dateninventar zu erstellen:

- **Produkt- und Dienstleistungsanalyse**: Es sollte das gesamte Portfolio geprüft werden, um festzustellen, welche Produkte als «vernetzte Produkte» und welche Dienstleistungen als «verbundene Dienste» im Sinne des Data Act gelten.
- **Datenklassifizierung**: Es sollte ein Inventar der Daten erstellt werden, die von diesen Produkten und Diensten generiert und abgerufen werden können. Dabei kann wie folgt unterschieden werden:
  - **Produktdaten/verbundene Dienstdaten (Rohdaten)**: Daten, die unter die Zugangs- und Herausgabepflichten fallen.
  - **Veredelte Daten**: Daten, die durch erhebliche Investition (z.B. mittels proprietärer Algorithmen) abgeleitet wurden und nicht herausgegeben werden müssen.
  - **Personendaten**: Daten, die einen Personenbezug aufweisen und zusätzlich den Regeln der DSGVO unterliegen.
  - **Geschäftsgeheimnisse**: Daten, deren Offenlegung einen wirtschaftlichen Schaden verursachen könnte.
- **Strategische Produktgestaltung («Access-by-Design»)**: Es sollte bewusst entschieden werden, welche Daten überhaupt extern abrufbar gemacht werden sollen. Nicht abrufbare Daten fallen nicht unter den Data Act. Es sollte erwogen werden, wertvolle Daten, die nicht geteilt werden sollen, bereits im Gerät so zu veredeln, dass sie von der Herausgabepflicht ausgenommen sind.

In einem zweiten Schritt sind die vertraglichen Grundlagen zu schaffen und anzupassen:

- **Herausgabe von Daten an Nutzer und Dritte (Art. 4 ff.) regeln**: Die Umsetzung der Herausgabepflicht kann vertraglich mit den Nutzern und bei Bedarf auch mit den Dritten geregelt werden, so unter anderem, um den Prozess zu regeln und Geschäftsgeheimnisse zu schützen. Es gibt hierfür Modellverträge, aber es kann auch mit eigenen Vorlagen gearbeitet werden.
- **Nutzungsrechte für Dateninhaber sichern (Art. 4(13))**: Die wichtigste vertragliche Massnahme ist die Sicherstellung der eigenen Nutzungsrechte. In Verträgen (AGB, Einzelverträge) sollten klare und transparente Klauseln ein-

44 Europäische Kommission, FAQ (Fn. 4), Frage Nr. 42a.

gebaut werden, die die Nutzung von Produkt- und Dienstdaten für eigene Zwecke (z.B. Produktverbesserung, Entwicklung neuer Dienste, Aggregation) gestatten.
- **Weitergaberechte regeln (Art. 4(14))**: Sofern Daten an Dritte (z.B. Komponentenhersteller, Analysepartner) weitergeben werden sollen, muss dies vertraglich explizit mit dem Nutzer vereinbart werden.
- **Vertragsketten sicherstellen**: Vertragspartner (z.B. Händler, Vermieter), sollten verpflichtet werden, die vorformulierten Nutzungs- und Weitergaberechte nachfolgenden Nutzern (Käufer, Mieter) zu überbinden. Ohne eine lückenlose Vertragskette kann die eigene Datennutzung unzulässig sein.
- **Weiterer Schutz von Geschäftsgeheimnissen**: Verträge sollten robuste Geheimhaltungsklauseln beinhalten, die auch den Umgang mit Produktdaten nach Art. 3(1) umfassen. Nutzungsbeschränkungen sollten erwogen und definiert werden, um die eigenen Interessen zu wahren.

In einem dritten Schritt sind die Prozesse für Informations- und Herausgabepflichten zu implementieren:
- **Bereitstellung vorvertraglicher Informationen (Art. 3(2) und 3(3))**: Es sollten die gesetzlich geforderten Informationsdokumente erstellt werden. Diese müssen vor Vertragsschluss zur Verfügung gestellt werden (z.B. in Offerten, AGB, auf einer verlinkten Webseite). Sicherzustellen ist auch, dass jeder in der Vertriebskette (z.B. auch das Autohaus bei einem Fahrzeugverkauf) seine eigene Informationspflicht erfüllt.
- **Prozess für Datenzugangsanfragen (Art. 4 und 5)**: Es sollte ein standardisierter Prozess eingerichtet werden, um Anfragen von Nutzern auf Datenherausgabe effizient zu bearbeiten. Dieser Prozess muss Folgendes umfassen:
  - Identifizierung des Anfragenden
  - Prüfung, ob die angefragten Daten erfasst sind
  - Identifizierung und Deklaration von Geschäftsgeheimnissen sowie die Vereinbarung von Schutzmassnahmen
  - Prüfung datenschutzrechtlicher Grundlagen, falls Personendaten von Dritten betroffen sind, und Einholung entsprechender Nachweise vom Anfragenden
  - Technische Bereitstellung der Daten im geforderten Format
- **Schnittstellen bereitstellen («Access-by-Design», Art. 3(1))**: Die Nutzer sollten grundsätzlich einen direkten, einfachen und kostenlosen Zugang zu den Rohdaten der vernetzten Produkte und verbundenen Dienste erhalten. Dies beinhaltet die Bereitstellung der notwendigen Metadaten und API-Dokumentationen, um die Daten interpretierbar und nutzbar zu machen. Diese Pflicht gilt allerdings erst ab dem 12. September 2026.

Im Rahmen dieser Schritte soll auch das Risikomanagement nicht zu kurz kommen, etwa durch entsprechende vertragliche Absicherungen beim Umgang mit Personendaten oder beim Schutz vor Missbrauch der Daten durch die Nutzer und Dritte.

XI. Fazit

Der Data Act stellt eine fundamentale Anpassung der Regelung der europäischen Datenwirtschaft dar, deren praktische Umsetzung jedoch erst am Anfang steht und von erheblicher Komplexität geprägt ist. Obwohl die Verordnung seit dem 12. September 2025 anwendbar ist, haben viele Unternehmen gerade erst begonnen, sich mit den Pflichten auseinanderzusetzen. Die vielen offenen Fragen sind einer raschen Umsetzung nicht zuträglich. Eine Bitkom-Studie im Frühjahr 2025 ergab für Deutschland, dass nur gerade jedes hundertste Unternehmen den Data Act vollständig umgesetzt hatte, und weitere vier Prozent immerhin teilweise.[45]

Ein zentrales Problem ist die Rechtsunsicherheit, die aus vielen unpräzise formulierten Legaldefinitionen resultiert. Schlüsselbegriffe wie «Produktdaten», «verbundener Dienst» oder «Dateninhaber» sind nicht klar. Diese Unschärfe wird dadurch verschärft, dass bislang kaum etablierte juristische Literatur oder Kommentierungen existieren, die eine verlässliche Auslegungshilfe bieten könnten. Selbst erste offizielle Hilfestellungen, wie die FAQ der Europäischen Kommission, gelten als lückenhaft.

Erforderlich ist daher, dass die erforderlichen Entscheide über die Produktgestaltung, die Datenklassifizierung und die Ausarbeitung von Vertragswerken risikobasiert getroffen werden. Es ist besser, eine nicht perfekte Produkteinformation nach Art. 3 oder eine Klausel zur eigenen Datennutzung nach Art. 4(13) bereits zu haben als abzuwarten, welche Standards sich etablieren. Umgekehrt dürfte in absehbarer Zeit noch nicht mit einer harten behördliche Durchsetzung zu rechnen sein. Druck dürfte – wenn überhaupt – primär von Anspruchsberechtigten kommen, die bei Unternehmen mit ihren Herausgabebegehren aufschlagen – und von Dritten, die ihre Geschäfte mit Hilfe des Data Acts ausbauen möchten, wie z.B. konkurrierende Wartungsanbieter.

45 ‹www.bitkom.org/Presse/Presseinformation/Data-Act-Fragen-bleiben-offen›, zuletzt abgerufen am 29. Oktober 2025.

Zusammenfassung

Der EU Data Act, der seit dem 12. September 2025 grösstenteils anwendbar ist, stellt eine neue Säule der EU-Digitalregulierung dar und verpflichtet Unternehmen zu weitreichenden Anpassungen. Im Kern gewährt die Verordnung den Nutzern von vernetzten Produkten und verbundenen Diensten umfassende Zugangs- und Kontrollrechte über die von diesen generierten Daten. Anbieter müssen durch «Access-by-Design» sicherstellen, dass Nutzer direkten und kostenlosen Zugang zu Rohdaten wie Sensor- oder Nutzungsdaten erhalten. Gleichzeitig wird die eigene Nutzung dieser Daten durch die Anbieter, die als «Dateninhaber» gelten, stark eingeschränkt und bedarf einer expliziten vertraglichen Vereinbarung mit dem Nutzer. Diese Pflichten betreffen nicht nur Hersteller, sondern die gesamte Lieferkette und sind auch für Schweizer Unternehmen relevant, die in den EU-Markt exportieren.

Die praktische Umsetzung des Data Acts ist mit erheblichen Herausforderungen und Rechtsunsicherheiten verbunden, die sich aus unklaren Definitionen von Schlüsselbegriffen wie «Produktdaten», «verbundener Dienst» oder «Dateninhaber» ergeben. Unternehmen müssen eine genaue Analyse ihres Portfolios vornehmen, um den Anwendungsbereich zu klären und die betroffenen Daten zu klassifizieren. Besondere Aufmerksamkeit erfordert der Schutz von Geschäftsgeheimnissen und der Umgang mit Personendaten, für die der Data Act spezifische Regelungen vorsieht. Die Herausgabepflichten gegenüber Nutzern und Dritten sowie die Sicherung eigener Nutzungsrechte erfordern die Implementierung neuer Prozesse und die Anpassung von Verträgen, um die Einhaltung der Vorschriften zu gewährleisten und Sanktionen, die sich am Bussenrahmen der DSGVO orientieren, zu vermeiden.

Résumé

Le règlement sur les données de l'UE (Data Act), qui est en grande partie applicable depuis le 12 septembre 2025, constitue un nouveau pilier de la réglementation numérique de l'UE et oblige les entreprises à procéder à des adaptations importantes. En substance, le règlement accorde aux utilisateurs de produits connectés et de services associés des droits d'accès et de contrôle étendus sur les données générées par ceux-ci. Les fournisseurs doivent garantir, par le biais de l'«Access-by-Design», que les utilisateurs aient un accès direct et gratuit aux données brutes telles que les données des capteurs ou les données d'utilisation. Dans le même temps, l'utilisation de ces données par les fournisseurs, qui sont considérés comme les «propriétaires des données», est fortement restreinte et nécessite un accord contractuel explicite avec l'utilisateur. Ces obligations concernent non seulement les fabricants, mais aussi l'ensemble de la chaîne d'approvisionnement et s'appliquent également aux entreprises suisses qui exportent vers le marché de l'UE.

La mise en œuvre pratique du règlement sur les données pose des défis considérables et entraîne des incertitudes juridiques qui découlent de la définition imprécise de termes clés tels que «données des produits», «service connecté» ou «propriétaire de données». Les entreprises doivent procéder à une analyse précise de leur portefeuille afin de clarifier le champ d'application et de classer les données concernées. Une attention particulière doit être accordée à la protection des secrets d'affaires et au traitement des données à caractère personnel, pour lesquels le règlement sur les données prévoit des règles spécifiques. Les obligations de divulgation envers les utilisateurs et les tiers ainsi que la protection des droits d'utilisation propres nécessitent la mise en œuvre de nouveaux processus et l'adaptation des contrats afin de garantir le respect des réglementations et d'éviter les sanctions, qui s'alignent sur le cadre des amendes prévues par le RGPD.

Inhaltsverzeichnis | Table des matières

Themenheft: Digitalisierung | Numéro spécial: numérisation

Aufsätze | Articles

Rechtsprechung | Jurisprudence

Bibliographie