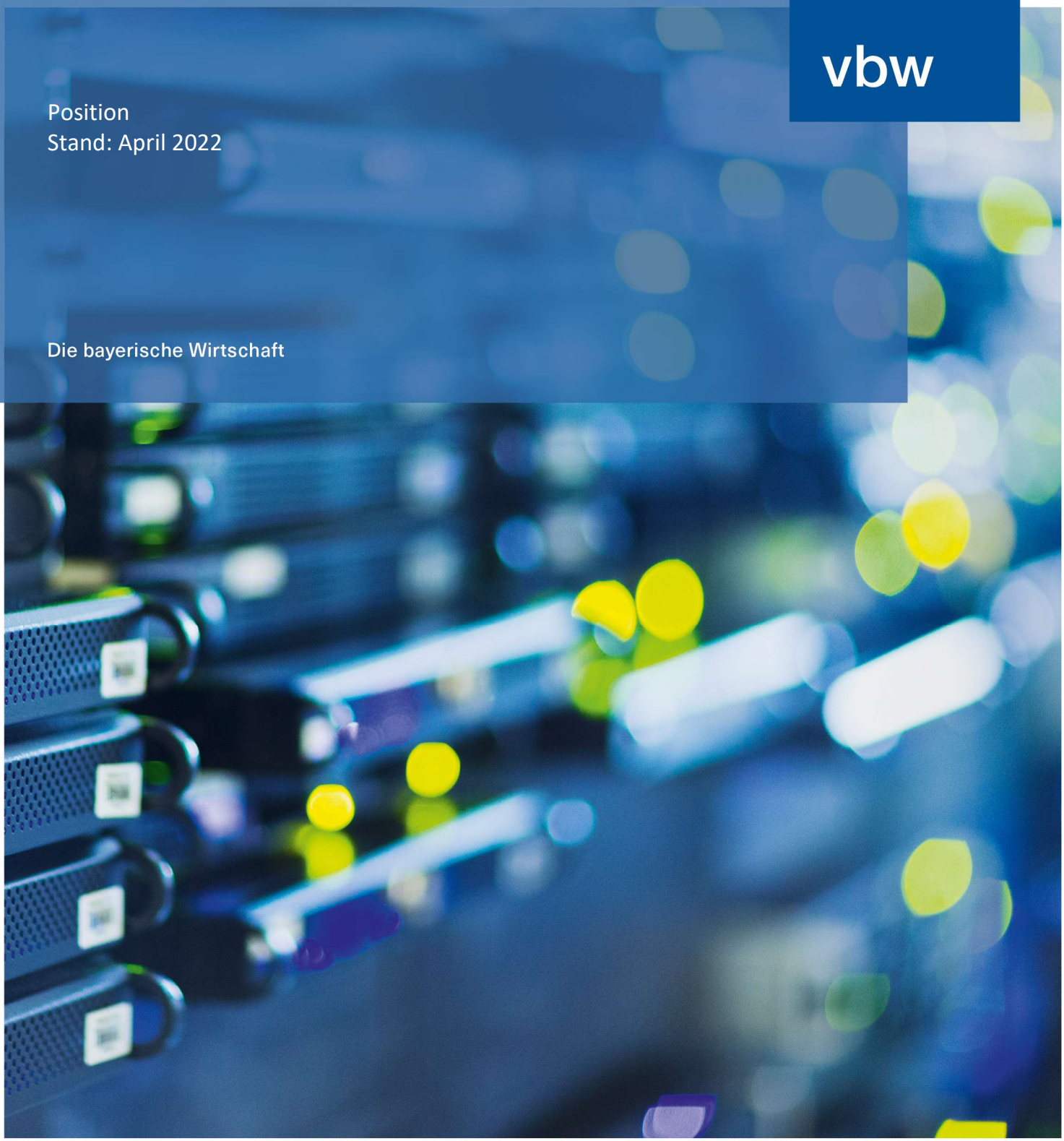
Digitalisierung

Data Act – Anpassungsbedarf aus Sicht der Bayerischen Wirtschaft

vbw

Position
Stand: April 2022

Die bayerische Wirtschaft



Hinweis

Vorwort

Mit dem Entwurf des Data Acts zur Schaffung harmonisierter Vorschriften für einen fairen Datenzugang und eine faire Datennutzung legt die EU-Kommission einen weiteren Baustein ihrer umfassenden Datenstrategie vor. So richtig das Ziel auch ist, eine starke europäische Datenwirtschaft aufzubauen, so kritisch sind teilweise die Mittel zu beurteilen.

Im Kern geht es darum, den Nutzern von vernetzten Produkten des „Internet der Dinge“ einen Anspruch auf Zugang zu den bei der Nutzung entstehenden Sachdaten zu gewähren. Diese Daten können sie auch Dritten zugänglich machen. Portabilität und Interoperabilität sollen gestärkt und der Wettbewerb dadurch gefördert werden. Soweit ist an der Grundidee wenig auszusetzen.

Der Entwurf der EU-Kommission geht jedoch deutlich darüber hinaus. Was sich in weiten Teilen liest wie eine Verbraucherschutzregelung, betrifft tatsächlich auch das Verhältnis zwischen Unternehmen (B2B). Ausnahmen für kleine und mittlere Unternehmen helfen nicht weiter, sondern verschärfen die bestehenden Asymmetrien, insbesondere auch zulasten der Industrie.

Die Bayerische Wirtschaft tritt dafür ein, dass der Entwurf im weiteren Gesetzgebungsverfahren auf seinen sinnvollen Kern zurückgeführt wird. Zusätzlich muss die Gelegenheit ergriffen werden, Klarstellungen im Datenschutzrecht vorzunehmen, statt die dortigen Zweifelsfragen in den Bereich der Sachdaten zu übertragen.

Bertram Brossardt
13. April 2022

Inhalt

Position auf einen Blick 1

1 Grundgedanken, Anwendungsbereich und Definitionen 2

1.1 Grundgedanken des Entwurfs 2

1.2 Bewertung 2
1.2.1 Zugrundeliegende Annahmen sind teilweise nicht nachvollziehbar 3
1.2.2 Differenzierung nach Unternehmensgröße passt schlecht zu den Gegebenheiten der Datenwirtschaft 4
1.2.3 Datenbegriff zu konturlos 4
1.2.4 Adressaten der Regulierung unpräzise definiert 5
1.2.5 Abgrenzungsprobleme des Datenschutzrechts fortgeschrieben 5
1.2.6 Fazit: Eine sachgerechte Begrenzung des Anwendungsbereichs ist erforderlich 6

2 Zugang zu Daten 7

2.1 Kerninhalt des Entwurfs 7

2.2 Bewertung 7
2.2.1 Ausgestaltung des Zugangs, Access by Design 7
2.2.2 Datenschutzrecht als Risiko 8
2.2.3 Zustimmung und Datennutzungsvereinbarung 9
2.2.4 Vorvertragliche Informations- und Transparenzpflichten 9
2.2.5 Wettbewerblicher Schutz 9
2.2.6 Schutz von Geschäftsgeheimnissen 10
2.2.7 Asymmetrische Regelung der Rechte und Pflichten 11

3 Vorgaben für Vertragsinhalte 12

3.1 Regelungen des Kapitels III: Pflichten der Dateninhaber 12
3.1.1 Kerninhalte des Entwurfs 12
3.1.2 Bewertung 12

3.2 Regelungen des Kapitels IV: Missbräuchliche Klauseln 13
3.2.1 Kerninhalte des Entwurfs 13
3.2.2 Bewertung 13

3.3 Datenbereitstellung für öffentliche Stellen und Forschung 14
3.3.1 Kerninhalt der Regelung 14
3.3.2 Bewertung 14

4 Weitere Regelungsinhalte 16

4.1 Wechsel zwischen Datenverarbeitungsdiensten 16
4.1.1 Kerninhalt der Regelung 16
4.1.2 Bewertung 16

4.2 Schutzvorkehrungen für nicht personenbezogene Daten im internationalen Umfeld 16
4.2.1 Kerninhalt der Regelung 16
4.2.2 Bewertung 17

4.3 Interoperabilität 17
4.3.1 Kerninhalt der Regelung 17
4.3.2 Bewertung 17

4.4 Anwendung und Durchsetzung 17

4.5 Ausnahme vom Datenbankschutzrecht 18
4.5.1 Kerninhalt der Regelung 18
4.5.2 Bewertung 18

4.6 Umsetzungszeitraum 18

Ansprechpartner / Impressum 19

Position auf einen Blick

Digitale Transformation nicht unter Regulierung ersticken

Zu Recht sieht die Europäische Kommission große wirtschaftliche Potenziale in einer intensiveren Nutzung von Sachdaten und will diese fördern. Grundsätzlich ist sind daher eine Harmonisierung des Datenrechts und die Stärkung von Interoperabilität und Portabilität sinnvolle Anliegen.

Die Probleme beginnen dort, wo es um eine vermeintlich faire Verteilung von Wertschöpfung geht und massive Eingriffe in die Vertragsfreiheit vorgenommen werden, die auf relativ eindimensionalen Annahmen basieren und wenig Rücksicht auf getätigte Investitionen und Innovationsanreize für die Industrie nehmen.

Das Teilen von Daten zwischen Unternehmen – unabhängig von deren Größe – muss freiwillig bleiben. Gerade in der Industrie müssen maßgeschneiderte vertragliche Lösungen möglich bleiben. Der Anwendungsbereich des Data Act ist entsprechend einzuschränken.

Sofern es bei einer Anwendung des Data Act auch auf B2B-Beziehungen bleibt, müssen die im Entwurf angelegten Asymmetrien beseitigt werden. Die Differenzierung zwischen KMU und Großunternehmen führt vielfach zu Wertungswidersprüchen.

Geschäftsgeheimnisse müssen gewahrt werden können. Bei Bedarf ist dazu die Definition um objektive Elemente zu ergänzen.

Viele Definitionen und Anforderungen sind noch zu vage und müssen präzisiert werden. So ist beispielsweise klarzustellen, dass mit „Daten“ lediglich Rohdaten gemeint sind.

Im vorliegenden Entwurf setzen sich die Anwendungsschwierigkeiten der DSGVO fort und werden im Bereich der Sachdaten um neue Rechtsunsicherheiten ergänzt. Zentral für den Erfolg der Datenwirtschaft ist es, bestehende Hemmnisse beispielsweise bei der Anonymisierung zu beseitigen und größtmögliche Klarheit zu schaffen. Das gilt es vorrangig anzupacken. Dazu muss neben dem Data Act auch die DSGVO angepasst werden.

Im weiteren Gesetzgebungsverfahren gilt es, sich auf den tatsächlichen Regulierungsbedarf zu fokussieren, um so einen wertvollen Beitrag zu einer wettbewerbsfähigen europäischen Datenwirtschaft zu leisten.

1 Grundgedanken, Anwendungsbereich und Definitionen

Der Entwurf geht teilweise von fragwürdigen Grundannahmen aus und unterlässt notwendige Klarstellungen

Mit dem Data Act („Datengesetz“ in der deutschen Sprachfassung) soll ein sektorübergreifender Rahmen für den Datenzugang und die Datennutzung geschaffen werden. Ziel ist es, eine gerechtere Verteilung der Wertschöpfung aus Daten auf die Akteure der Datenwirtschaft zu gewährleisten und den Datenzugang sowie die Datennutzung zu fördern. Dazu soll unter anderem das Vertragsrecht angepasst werden. Es gilt das Marktortprinzip.

1.1 Grundgedanken des Entwurfs

Im Kern geht es um Daten, die im Zusammenhang mit dem Internet der Dinge erzeugt werden, also beispielsweise im Auto oder im Smart Home. Es gibt grundsätzlich vier mögliche Zugangsberechtigte, die unter bestimmten Voraussetzungen einen Zugriff auf bei der Nutzung eines Produkts oder damit verbundenen Dienstes entstehende Daten beanspruchen können:

- Nutzer des Produkts oder des Services (z. B. der Halter/Fahrer des Autos), die natürliche oder juristische Personen sein können,
- Dritte (natürliche oder juristische Person), sofern es sich nicht um bestimmte große Plattformunternehmen (sog. „Gatekeeper“) handelt,
- Staatliche Stellen,
- Forschungseinrichtungen.

Anspruchsgegner ist ein Unternehmen, das kein KMU ist, und faktisch Zugriff auf die mit dem Produkt oder der Dienstleistung erzeugten Daten hat.

Von der Idee eines Dateneigentums hat sich die KOM verabschiedet. Nunmehr geht es um die Zuordnung von Verwendungsrechten, wobei ganz klar der Nutzer im Fokus steht, der ein Produkt oder eine Dienstleistung nutzt und dabei Daten erzeugt. Basis für die Verwendung sollen generell Verträge sein, wobei nur teilweise frei über den Abschluss und Inhalt entschieden werden kann.

1.2 Bewertung

Dass es an Daten in der EU auch künftig kein Eigentum oder eigentumsähnliches Recht geben soll ist richtig, war aber seit längerem auch nicht anders zu erwarten. Grundsätzlich entspricht es unserer Position, den Zugang zu Sachdaten auf vertraglicher Basis zu regeln –

aber freiwillig, also ohne Kontrahierungszwang, und ohne neue regulative Beschränkungen auch im B2B-Bereich. Dem wird der Entwurf nicht gerecht.

1.2.1 Zugrundeliegende Annahmen sind teilweise nicht nachvollziehbar

Zuzustimmen ist der EU in ihrer grundsätzlichen Analyse insoweit, als sich bisher keine ausreichende Dynamik in der europäischen Datenwirtschaft entwickelt hat. Die Gründe dafür sind allerdings zumindest teilweise anders gelagert, als in den vorgeschalteten Erwägungen suggeriert wird.

Die Grundannahmen, von denen die KOM hier ausgeht, sind kritisch zu hinterfragen. Anhand ihrer Konsultation geht sie davon aus, dass das Teilen von Daten zwischen Unternehmen gängige Praxis sei. Das entspricht nicht den Ergebnissen, die aus Erhebungen folgen, die deutlich repräsentativer sind als die Rückmeldungen im Rahmen der Konsultation: Während sich dort lediglich 105 Unternehmen und Unternehmensverbände beteiligt hatten (was naturgemäß auch an der Bündelungsfunktion von Verbänden liegt), zeigte beispielsweise unsere Befragung von 425 bayerischen Unternehmen aus Industrie und industrienahen Dienstleistungen (*Digitalisierung der Unternehmen in Bayern*, IW Consult, Januar 2022), dass vertragliche Nutzungsvereinbarungen über Daten zwischen Unternehmen sehr wenig verbreitet sind. Die Anteile der Unternehmen, die solche Vereinbarungen beim Bezug von Daten geschlossen haben, schwanken von 1,8 Prozent im Bereich der Kundendaten bis 11,3 Prozent für Produktdaten. Auch die Angaben zum Einsatz von KI und weiteren digitalen Technologien liegen bei der KOM weit über denen unserer verschiedenen Erhebungen.

70 Prozent der Interessensträger haben laut Kommission angegeben, dass es bei Daten, die im Zusammenhang mit dem Internet der Dinge ein Fairnessproblem gebe und es dem Hersteller nicht möglich sein dürfe, alleine darüber zu entscheiden, was mit diesen Daten geschieht. Eine Verzerrung ist hier strukturell angelegt, weil Zulieferer und Kunden weit überrepräsentiert sind und nur nach dem Hersteller gefragt wurde – ob dieser tatsächlich Zugang zu den Daten hat, ist eine ganz andere Frage.

Was dagegen fehlt, sind Hemmnisse, die aus Rechtsunsicherheiten entstehen. Diese sind tatsächlich dominant: 82 Prozent der bayerischen Unternehmen nennen in der oben genannten Studie datenschutzrechtliche Grauzonen, 76 Prozent die fehlende Rechtssicherheit bei der Anonymisierung als Grund dafür, dass sie Sachdaten nicht intensiver wirtschaftlich nutzen. Die deutschlandweiten Ergebnisse sind sehr ähnlich (vgl. *Datenwirtschaft in Deutschland*, IW, Februar 2021).

Diese Grundannahmen führen letztlich dazu, dass die KOM im Entwurf eine klar asymmetrische Regelung vorlegt, die so die Praxis nur sehr unzureichend abbilden kann.

1.2.2 Differenzierung nach Unternehmensgröße passt schlecht zu den Gegebenheiten der Datenwirtschaft

Große Unternehmen sind nicht per se mächtig und kleine nicht per se schutzbedürftig in dem hier betrachteten Bereich. Gerade im IT-Bereich darf als bekannt vorausgesetzt werden, dass zahlreiche datengestützte Innovationen auf Start-ups zurückzuführen sind, die bei entsprechendem Markterfolg teilweise zwar schnell wachsen, vielfach aber angesichts der Skalierbarkeit digitaler Anwendungen nicht in gleichem Maße und Tempo Personal aufbauen. Im industriellen Bereich konnten bisher keine strukturellen Ungleichgewichte identifiziert werden. Insbesondere haben sich auch keine marktbeherrschenden Plattformen herausgebildet. Es spricht wenig dafür, dass sich das ändert. Wo es tatsächlich eindeutig ein ungleiches Kräfteverhältnis gibt – insbesondere bei Mobile Devices (beispielsweise Smartphones) – soll die Neuregelung dagegen gar nicht eingreifen.

Wenn man der Grundüberlegung der KOM folgt, dass auch in den B2B-Bereich hineinreguliert werden muss, dann kann es durchaus auch umgekehrt angebracht sein, ein mit datengetriebenen Geschäftsmodellen unerfahrenes Großunternehmen vor aggressiven Praktiken eines kleinen spezialisierten IT-Unternehmens zu schützen. Die Unterscheidung zwischen KMU und Großunternehmen ist im Kontext der Datenwirtschaft daher als pauschales Differenzierungskriterium ungeeignet.

1.2.3 Datenbegriff zu konturlos

Nach Art. 2 Nr. 1 ist unter „Daten“ im Sinne der Verordnung jede digitale Darstellung von Handlungen, Tatsachen oder Informationen sowie jede Zusammenstellung solcher Handlungen, Tatsachen oder Informationen zu verstehen, auch in Form von Ton-, Bild- oder audiovisuellem Material.

Der Anwendungsbereich ist damit viel zu wenig eingegrenzt. Schon aus den Erwägungsgründen wird deutlich, dass jedenfalls aus Daten abgeleitete oder gefolgerte Informationen, sofern sie rechtmäßig erlangt wurden, nicht in den Anwendungsbereich der Verordnung fallen sollen. Diese Abgrenzung sucht man im eigentlichen Verordnungstext aber vergeblich. Das muss ergänzt werden. Richtig wäre die Klarstellung, dass es beim Zugangsanspruch lediglich um Rohdaten geht.

Auch unabhängig davon ist aber eine klare Differenzierung erforderlich. Nicht erfasst werden dürfen Daten, die unabhängig von der konkreten Nutzung entstehen (beispielsweise im Zusammenspiel verschiedener Komponenten), weil hier schon nicht ersichtlich ist, welches schutzwürdige Interesse der Nutzer daran haben könnte, weswegen er an einer Wertschöpfung zu beteiligen wäre. Für ein solches Verständnis spricht die Formulierung in Art. 3 Abs. 1 und Art. 4 Abs. 1, die von den „bei der Nutzung erzeugten“ Daten sprechen, macht das aber nicht hinreichend deutlich.

Unklar ist ferner, wie mit flüchtigen Daten umzugehen ist, etwa mit solchen, die zwar theoretisch (etwa durch den Einsatz von Sensoren) entstehen, aber gar nicht ausgelesen

werden, weil das zu aufwendig wäre. Grundsätzlich darf sich der Anspruch darauf nicht erstrecken, da anderenfalls auf Kosten (und ggf. Risiko) des Herstellers eine Schnittstelle beziehungsweise Speichermöglichkeit geschaffen werden müsste. Allenfalls kann dies einem Dritten oder dem Nutzer (auf deren Kosten) ermöglicht werden.

1.2.4 Adressaten der Regulierung unpräzise definiert

Der Verordnungsentwurf geht von einem stark simplifizierenden Verständnis von den Beziehungen zwischen Hersteller und Kunden aus. Es wird an vielen Stellen sichtbar, dass nur einige wenige Fallkonstellationen betrachtet wurden, die Komplexität der Praxis jedoch nicht abgebildet werden kann.

– So kann beispielsweise der „Nutzer“ bereits eine Verfügungsmöglichkeit über die von ihm „erzeugten“ Daten haben und es kann mehrere Nutzer geben (zum Beispiel Mieter und Vermieter). Im Hinblick auf Services fehlt außerdem die nach den Erwägungsgrund 18 offenbar (zu Recht) gewollte Eingrenzung, dass es sich um eine Nutzung auf vertraglicher Basis handeln muss.
– Auch auf Seiten des „Dateninhabers“ ist dementsprechend keineswegs eindeutig, wer das in der konkreten Konstellation ist. Dateninhaber ist nach Art. 2 Nr. 6, wer durch die Kontrolle über die technische Konzeption des Produkts und damit verbundener Dienste in der Lage ist, bestimmte Daten bereitzustellen. Aus den Erwägungsgründen entsteht der Eindruck, dass das aus der Perspektive der Kommission ganz regelmäßig der Hersteller des Produkts ist. Tatsächlich können das aber durchaus ebenfalls verschiedene Unternehmen sein (neben dem Hersteller zum Beispiel Zulieferer von Komponenten, Verkäufer, Anbieter von verbundenen Dienstleistungen), die auf verschiedenen Ebenen Einfluss nehmen können – oder auch nicht mehr – und vertragliche Regelungen miteinander und mit Dritten getroffen haben können.

Wenn aber bereits die Adressaten der Regelungen unklar sind, ist eine sinnvolle Umsetzung unmöglich.

1.2.5 Abgrenzungsprobleme des Datenschutzrechts fortgeschrieben

Die Regelungen der DSGVO sollen durch den vorliegenden Entwurf nicht berührt werden (Art. 1 Abs. 3). Der Data Act ordnet das Recht zur Entscheidung über die Verwendung von Sachdaten im Wesentlichen dem Nutzer zu (der allerdings auch ein Unternehmen sein kann). Faktisch würde der Data Act in der vorliegenden Form dazu führen, dass Sachdaten einem durchaus ähnlichen Regime unterliegen wie personenbezogene – aber nicht demselben, so dass die Abgrenzungsprobleme noch weitere Kreise ziehen. Ein praktisches Problem dürfte ferner darin liegen, dass es oftmals um gemischte Datensatze (teilweise mit Personenbezug, teilweise ohne, teilweise wohl auch mit unklarer Zuordnung) geht.

Hier besteht dringender Handlungsbedarf. Es kann nicht angehen, dass bestehende Anwendungsschwierigkeiten einfach in immer neuen Regelungen fortgeschrieben werden. Zu den wesentlichen Hemmnissen für eine intensivere Nutzung von Sachdaten zählen datenschutzrechtliche Grauzonen und fehlende Rechtssicherheit bei der Anonymisierung. Diese

Hemmnisse müssen zuerst angepackt werden, und zwar durch Klarstellungen in der DSGVO, wenn die Datenwirtschaft gefördert werden soll.

1.2.6 Fazit: Eine sachgerechte Begrenzung des Anwendungsbereichs ist erforderlich

Das Teilen von Daten zwischen Unternehmen – unabhängig von deren Größe – muss freiwillig bleiben. Ein bloßes geschäftliches Interesse Dritter kann auch mit der Billigung des Nutzers als weiterem Beteiligten noch keinen Kontrahierungszwang zwischen Unternehmen rechtfertigen, der in unserer von der Vertrags- und Abschlussfreiheit geprägten Rechtsordnung eine absolute Ausnahme darstellen muss. Der Anwendungsbereich des Data Act ist entsprechend einzuschränken.

Wenn sich im Einzelfall tatsächlich massive Ungleichgewichte zeigen sollten, kann mit den Instrumenten des Wettbewerbsrechts gegengesteuert oder unter Umständen auch eine sektorspezifische Regelung erlassen werden. Allenfalls im Hinblick auf heute schon der Datenwirtschaft zuzurechnende große Unternehmen (insbesondere die im Entwurf genannten Gatekeeper) wäre eine B2B-Regelung mit der Begründung denkbar, hier eine gewisse Waffengleichheit herzustellen.

2 Zugang zu Daten

Erhebliche Asymmetrie bei den Rechten und Pflichten

2.1 Kerninhalt des Entwurfs

Hersteller und Entwickler müssen ihre Produkte so gestalten, dass die Daten standardmäßig leicht zugänglich sind, und sie müssen offenlegen, welche Daten zugänglich sind und wie darauf zugegriffen werden kann (vorvertragliche Transparenz- und Informationspflichten).

Der Nutzer kann Zugriff auf die Daten für sich selbst verlangen, oder für einen von ihm bestimmten Dritten.

In diesem Kapitel II des Entwurfs findet keine Unterscheidung zwischen der Datenweitergabe von Unternehmen an Verbraucher und zwischen Unternehmen statt; der Nutzer kann immer beides sein. Eine Ausnahme hinsichtlich der Pflichten greift für KMU; sog. Gatekeeper im Sinne des Gesetzes über digitale Märkte kommen nicht als „Dritte“ in Betracht.

2.2 Bewertung

2.2.1 Ausgestaltung des Zugangs, Access by Design

Nach Art. 3 Abs. 1 sind Produkte so zu konzipieren und herstellen und verbundene Dienste so zu erbringen, dass die bei ihrer Nutzung erzeugten Daten standardmäßig für den Nutzer einfach, sicher und – soweit relevant und angemessen – direkt zugänglich sind (Access by Design). Wenn kein Zugriff vom Gerät selbst aus möglich ist, muss der Dateninhaber eine Infrastruktur vorhalten, mit der er dem Nutzer die bei der Nutzung erzeugten Daten „unverzüglich, kostenlos und gegebenenfalls kontinuierlich und in Echtzeit“ zur Verfügung stellt (Art. 4 Abs. 1).

Diese sehr weite Formulierung ist für die Praxis nicht tauglich. Es bleibt vollkommen offen, wie weit die Verpflichtung geht, ob sie sich also beispielsweise auch auf solche Daten erstrecken soll, die bisher weder gespeichert noch sonst in irgendeiner Weise genutzt wurden und für deren Nutzung auch keine Vorkehrungen getroffen worden sind (vgl. auch oben). Damit der Nutzer „sicher“ auf Daten zugreifen kann, deren Auslesen bisher überhaupt nicht vorgesehen war, müssten gegebenenfalls ganz neue Systeme vorgesehen werden, mit den entsprechenden Kostenfolgen. Offen bleibt auch, was unter „zugänglich“ zu verstehen ist: ist dazu eine Übermittlung erforderlich, oder genügt auch ein Lesezugriff? Es kann im Einzelfall sachgerecht sein, die Daten im Gerät zu belassen, und auch das muss ohne weiteres zulässig sein. Schließlich muss das Verhältnis von Art. 3 Abs. 1

(standardmäßig einfacher Zugang) und Art. 4 Abs. 1 (kein Zugriff direkt vom Produkt aus möglich) geklärt werden: aktuell kann es so gelesen werden, als sei Art. 4 Abs. 1 eine Ausnahme von Art. 3 Abs. 1, obwohl es offenbar als andere legitime Form der Ausgestaltung des Zugriffs gemeint ist. Regelungstechnisch gehört diese Ausgestaltungsvariante wohl in Art. 3.

Schon das Schaffen einer Zugangsmöglichkeit kann als solches sicherheitsrelevant sein. Hinzu kommen die Fragen möglicher Haftungsansprüche, eines Regresses innerhalb der Lieferungs- beziehungsweise Wertschöpfungskette und die generelle Bußgeldbewehrtheit der Pflichten aus dem Entwurf. Alle diese Fragen müssen für den Dateninhaber klar geregelt sein. Anderenfalls kann die Konsequenz sein, dass weniger digitale Technologien verbaut und weniger Daten erzeugt werden – oder wie es ein Unternehmensvertreter formulierte: dann müssten wir unsere Produkte und Anlagen absichtlich dümmer machen

Anforderungen an die Konstruktion der Produkte und Services müssen daher engsten Grenzen unterliegen, zumal die Kosten allenfalls teilweise über den Preis des Produkts oder des Services umgelegt werden können, danach aber allenfalls noch sehr beschränkt.

Nicht nur für KMU – die von den Verpflichtungen auch deshalb befreit sind – würde es eine erhebliche Belastung darstellen, die Anforderungen der Verordnung zu erfüllen, sondern auch für die meisten größeren Unternehmen. Das gilt besonders für Produkte, die nicht in großer Stückzahl hergestellt werden, und generell für Unternehmen, die aus unterschiedlichen Gründen nicht die Möglichkeit haben, zusätzliche Entwicklungs- und Bereitstellungskosten über höhere Preise im Markt durchzusetzen. Der Anwendungsbereich sollte daher auf B2C-Beziehungen beschränkt werden. Als Kompromiss ist allenfalls denkbar, nur in Bezug auf (Sach-)Daten besonders marktmächtige Unternehmen Zugangsregeln zu definieren; in der Logik des Entwurfs müssten das die sog. Gatekeeper sein. Auch diesbezüglich gilt es allerdings noch einmal nachzuschärfen (in diesem Fall im Digital Markets Act), um angemessen auf hierzulande noch unbekannte außereuropäische Wettbewerber reagieren zu können.

2.2.2 Datenschutzrecht als Risiko

Nach dem Entwurf läuft der Dateninhaber permanent Gefahr, gegen die DSGVO zu verstoßen, um einem Zugangsverlangen zu entsprechen. Er stünde also zwischen zwei in unterschiedlichen Verordnungen jeweils sanktionsbewehrten Pflichten, ohne dafür auch nur eine Ursache gesetzt zu haben. Der Entwurf löst diese Problematik nicht auf: so regelt etwa Art. 5 Abs. 1 die Pflicht zur unverzüglichen Weitergabe von Daten an einen Dritten auf Verlangen des Nutzers, während Art. 5 Abs. 9 lapidar feststellt, dass dadurch nicht die Datenschutzrechte anderer Personen beeinträchtigt werden dürfen.

Richtig wäre eine gesetzgeberische Klarstellung in der DSGVO und/oder im Data Act, etwa durch die Schaffung einer eigenständigen Rechtsgrundlage für die Verarbeitung personenbezogener Daten. Mindestanforderung ist es, dem Dateninhaber nicht das Risiko einer Fehleinschätzung aufzubürden, etwa im Hinblick auf die Gerichtsfestigkeit der

Anonymisierung oder die korrekte datenschutzrechtliche Beurteilung des Sachverhalts. Es muss zudem eindeutig formuliert werden, dass sich Zugangsansprüche nicht auf personenbezogene oder personenbeziehbare Daten anderer Betroffener erstrecken.

2.2.3 Zustimmung und Datennutzungsvereinbarung

Der Dateninhaber darf die bei der Nutzung erzeugten Sachdaten nur auf Grundlage einer vertraglichen Vereinbarung mit dem Nutzer verwenden (Art. 4 Abs. 6). Auch der Dritte darf die Daten nur für die Zwecke und unter den mit dem Nutzer vereinbarten Bedingungen verwenden (Art. 6). Insofern besteht eine Nähe zur Einwilligung nach der DSGVO. Allerdings ist die Zustimmung des Nutzers als einmalige, nicht widerrufliche Erklärung gedacht, wie auch der Vergleich zur Zustimmung des Dritten in Art. 5 Abs. 5 zeigt – das sollte im Text noch deutlicher gemacht werden.

Ungeregelt ist aber, welche Auswirkungen die Beendigung eines Vertrags bei den verschiedenen Beteiligten auf die bereits erlangten Daten hat. Für die Zukunft wird jedenfalls eine neue Vereinbarung notwendig sein.

Datennutzungsvereinbarungen müssen auch innerhalb der Vertragslaufzeit hinreichend flexibel sein beziehungsweise formuliert werden dürfen, da sich der Zweck bei langlebigen Produkten durchaus mehrfach ändern kann. Hier jeweils neu zu verhandeln ist wenig praktikabel. Die enge Zweckbindung des Datenschutzrechts sollte nicht auf Sachdaten übertragen werden, zumal der Gesetzgeber hier ja gerade eine möglichst breite (und wenig sparsame) Nutzung anstrebt. Vor diesem Hintergrund kann auch hinterfragt werden, warum der Dritte nach Art. 6 Abs. 2c) die erhaltenen Daten nicht nur – zu Recht – nicht als Rohdaten weitergeben darf, sondern auch nicht in aggregierter oder abgeleiteter Form, also gegebenenfalls mit einem eigenen Wertschöpfungsbeitrag.

2.2.4 Vorvertragliche Informations- und Transparenzpflichten

Transparenzpflichten werden in ihrer Wirkung auf den Bürger regelmäßig stark überschätzt. Wenn es sich beim Nutzer um einen Verbraucher handelt, wird er vielfach selbst mit den Informationen wenig anfangen können. Tatsächlich profitieren hier lediglich Unternehmen davon, und dabei insbesondere (potenzielle) Wettbewerber. Dementsprechend zurückhaltend müssen die entsprechenden Pflichten auch in Anbetracht des zusätzlichen Aufwands für die Aufbereitung der Informationen ausgestaltet werden, was gegenwärtig nicht der Fall ist.

2.2.5 Wettbewerblicher Schutz

Dass es dem Dritten nach dem Entwurf untersagt sein soll, die Daten zur Entwicklung eines konkurrierenden Produkts zu nutzen (Art. 6 Abs. 2 e)), ist von der Intention her richtig. Es wäre jedoch zu kurz gesprungen, wenn davon nur physische Produkte erfasst würden – ein

Schutz ist auch im Hinblick auf konkurrierende Dienstleistungen und Software notwendig. Wenn der europäische Gesetzgeber hier unbedingt die Möglichkeit konkurrierender Angebote schaffen will, dann muss er mindestens eine Definition aufnehmen, die das Missbrauchspotenzial eindämmt. Dazu kann auch eine angemessene Beteiligung des ursprünglichen Entwicklers am wirtschaftlichen Erfolg der „Kopie“ zählen.

Die Verordnung soll gezielt die europäische Datenwirtschaft im Verhältnis zu den außereuropäischen Wettbewerbern stärken. Unklar ist allerdings, wie verhindert werden sollte, dass so ein Wettbewerber eine europäische Tochter alleine mit dem Zweck gründet, sich Zugang zu Daten zu verschaffen – im Falle eines KMU sogar fast kostenlos.

Größtes Einzelhemmnis für eine intensivere wirtschaftliche Nutzung von Daten ist unserer eingangs genannten Umfrage zufolge mit mehr als 90 Prozent die Sorge vor dem unautorisierten Zugriff Dritter. Dem kann nicht mit dem Argument begegnet werden, der Zugriff sei dann ja künftig nach dem Data Act legitimiert. Diese Sorge gilt es vielmehr ernst zu nehmen. Anderenfalls droht eine noch größere Zurückhaltung.

2.2.6 Schutz von Geschäftsgeheimnissen

Geschäftsgeheimnisse des Dateninhabers werden unzureichend geschützt. Der Entwurf schießt – in dem Bestreben, möglichst viele Daten zugänglich zu machen und dazu Gegenargumente weitestgehend auszuräumen – deutlich über das Ziel hinaus. In Art. 4 Abs. 3, also im Verhältnis zum Nutzer, heißt es, dass Geschäftsgeheimnisse nur offengelegt werden, wenn „alle besonderen Maßnahmen getroffen worden sind, die erforderlich sind, um die Vertraulichkeit (…) insbesondere gegenüber Dritten zu wahren.“ Ähnlich regelt es Art. 5 Abs. 8 im Verhältnis zu Dritten. Was das für Maßnahmen sein sollen, bleibt völlig offen. Der Dateninhaber kann nicht unter Hinweis auf bestehende Geschäftsgeheimnisse den Datenzugang verweigern. Begründet wird das mit der subjektiven Definition des Geschäftsgeheimnisses im europäischen Recht: anderenfalls hätte es der Dateninhaber in der Hand, ganze Gruppen von Daten auszunehmen.

Unklar ist außerdem, wie es forschenden Unternehmen gelingen kann, bei der Einbindung von Dienstleistern sich den exklusiven Zugriff auf die Daten zu sichern. Nach dem Wortlaut der Verordnung wäre nämlich der Dienstleister der Dateninhaber und als solcher gegebenenfalls zur Herausgabe verpflichtet. Dass das forschende Unternehmen alle Leistungen selber ausführen könnte, ist kein valides Gegenargument – die Arbeitsteilung in Wertschöpfungsketten hat sich bewährt und darf nicht behindert oder zerschlagen werden. Ein vergleichbares Problem stellt sich bei der Entwicklung von Prototypen beim Kunden. Dazu ist eine Klarstellung erforderlich – entweder im Rahmen der Definition des Nutzers oder als Ausnahmeregelung in Art. 4 und 5.

Ein angemessenes Schutzniveau wird auch nicht durch die Regelungen etwa zum Verbot der Datennutzung für die Entwicklung von Konkurrenzprodukten erstellt (siehe dazu oben), zumal die Einhaltung der entsprechenden Vorgaben für den Dateninhaber praktisch nicht kontrollierbar ist und entsprechende Schadensersatzansprüche oder auch

Sanktionen bei unzureichendem Schutz der Geschäftsgeheimnisse durch den Nutzer nicht vorgesehen sind.

Jedes Zugangsrecht muss dort seine Grenze finden, wo Geschäftsgeheimnisse betroffen sind. Das muss in der Verordnung ebenso klar geregelt werden, wie in Bezug auf das Datenschutzrecht. Wenn die europäische Definition des Geschäftsgeheimnisses als Anknüpfungspunkt ungeeignet ist, dann ist es diese, die angepasst und um objektive Kriterien ergänzt werden muss.

2.2.7 Asymmetrische Regelung der Rechte und Pflichten

Der Dateninhaber darf Daten nur auf Grundlage einer vertraglichen Vereinbarung mit dem Nutzer nutzen – ein Kontrahierungszwang ist insoweit (anders als umgekehrt) aber nicht ersichtlich. Dabei kann er ebenfalls ein erhebliches Interesse an den Nutzungsdaten haben, um zum Beispiel sein Produkt weiterzuentwickeln oder neue Services dafür anzubieten, was ebenfalls geeignet wäre, die Datenwirtschaft zu fördern. Den Hersteller treffen also Pflichten beim Design des Produkts, aber er kann sich nicht selbst ein Nutzungsrecht an den Daten oder – nicht zuletzt dank der unscharfen Definition – auch nur einer bestimmten Teilmenge an Daten verschaffen.

Der Dateninhaber darf die Daten auch nicht verwenden, um Einblicke in die wirtschaftliche Lage, Vermögenswerte und Produktionsmethoden des Nutzers oder in die Nutzung durch den Nutzer zu erlangen, wenn dies die gewerbliche Position des Nutzers auf den Märkten, auf denen er tätig ist, untergraben könnte. Gleiches gilt für das Verhältnis des Dateninhabers zum Dritten. Umgekehrt ist der Dritte aber nicht daran gehindert, aus den Daten Schlüsse über den Nutzer oder Dateninhaber zu ziehen, was bei einem Vergleich der von verschiedenen Dateninhabern bereitgestellten Datensätze durchaus möglich sein dürfte.

Solange die Verordnung auch den B2B-Bereich voll erfasst, läuft eine solche Einbahnstraße dem damit verfolgten Ziel zuwider, die europäische Datenwirtschaft insgesamt zu stärken. Es muss hier in jede Richtung „Waffengleichheit“ hergestellt werden.

3 Vorgaben für Vertragsinhalte

Der Data Act hat den Anspruch, weit über seinen Kernbereich hinaus Grundregeln zu definieren.

3.1 Regelungen des Kapitels III: Pflichten der Dateninhaber

3.1.1 Kerninhalte des Entwurfs

Für sämtliche Verpflichtungen zur Bereitstellung von Daten gilt: Alle Bedingungen für die Bereitstellung von Daten müssen fair und nicht diskriminierend und alle Gegenleistungen angemessen sein. Von KMU zu erbringende Gegenleistungen dürfen die Kosten der Bereitstellung nicht übersteigen (Art. 9 Abs. 2). In sektorspezifischen Regelungen (z. B. im Mobilitätsbereich) kann von Letzterem abgewichen werden. Ansonsten sollen die Regelungen von Kapitel III des Entwurfs grundsätzlich auch für künftiges sektorielles Datenzugangsrecht gelten.

3.1.2 Bewertung

Die Regelung zur angemessenen Gegenleistung ist in ihrer Unbestimmtheit problematisch und im Hinblick auf die Ausnahme für KMU nicht sachgerecht.

Die Frage der Angemessenheit der Gegenleistung ist aus dem Urheberrecht bekannt und dort seit rund 50 Jahren ungeklärt.

Die Konstruktion des Entwurfs zielt darauf ab, mehr Wettbewerb auf nachgelagerten Märkten zu schaffen. Damit ist der Dateninhaber auch dann verpflichtet, seinen (potenziellen) Wettbewerbern Daten zur Verfügung zu stellen, wenn er selbst darauf gestützte Services anbietet. Hier greift bisher (zu Unrecht) auch der Konkurrenzschutz nicht. Wenn er selbst sein Geschäftsmodell „aufsplittet“, muss er das Diskriminierungsverbot beachten, dem Dritten also Daten zu denselben Konditionen zur Verfügung stellen, wie er es konzernintern tut.

Wenn der Dateninhaber ein KMU ist, dann ist er zwar nach dem Entwurf nicht verpflichtet, Zugang einzuräumen. Tut er es aber doch, dann ist nicht nachvollziehbar, warum er mit einem weiteren KMU als Vertragspartner nicht einen angemessenen Gewinn dabei erzielen sollte. Art. 9 beschränkt den Anwendungsbereich auch nicht auf Konstellationen, in denen eine Pflicht zum Datenteilen besteht. Das wäre als absolutes Minimum vorzusehen, um nicht Verträge in der gesamten europäischen Datenwirtschaft zu beeinträchtigen.

Die vermeintlich *faire Aufteilung der Wertschöpfung* fußt offenbar auf einem Missverständnis. Was es allenfalls zu verteilen gibt, ist die faire Chance *auf* Wertschöpfung unter

Nutzung von Daten. Alles, was an Werten bereits geschaffen worden ist, muss davon ausgeklammert bleiben und steht demjenigen oder den Unternehmen zu, die das mit ihren Investitionen (beispielsweise in die Entwicklung des Produkts oder des Dienstes) und gegebenenfalls auch im Rahmen bestehender Vertragsbeziehungen erreicht haben. Diesem Anspruch wird der Entwurf nicht gerecht.

Was *Fairness* eigentlich bedeutet, beantwortet der Entwurf nicht. Bei richtigem Verständnis muss es darum gehen, dass jeder im Verhältnis seines Beitrags (Investitionen z. B. in die Entwicklung eines Produkts) aber auch seiner Verantwortung (z. B. für die Sicherheit, die Reparaturfähigkeit etc.) Werte schaffen und davon profitieren kann. Daraus folgt,

– dass der Hersteller / Dateninhaber nicht gezwungen werden darf, (potenziellen) Wettbewerbern Daten günstiger zur Verfügung zu stellen, als mit ihm verbundenen Unternehmen (die nicht unter die KMU-Definition fallen)
– dass er nicht dazu verpflichtet werden kann, Strukturen vorzuhalten, deren Kosten nicht auf den Dritten umgelegt werden können
– dass Unternehmen unabhängig von der Anzahl der Beschäftigten den gleichen Regelungen unterliegen müssen (hier: Angemessenheit der Gegenleistung).

3.2 Regelungen des Kapitels IV: Missbräuchliche Klauseln

3.2.1 Kerninhalte des Entwurfs

In Verträgen zwischen Unternehmen über die gemeinsame Datennutzung soll eine spezielle Missbrauchskontrolle verhindern, dass KMU einseitig missbräuchliche Vertragsklauseln auferlegt werden. Diese Regelungen sollen über den Regelungsbereich des Data Acts hinaus auch für künftiges sektorielles Datenzugangsrecht gelten.

Die Prüfung erstreckt sich nur auf die Klauseln, die tatsächlich den Datenzugang regeln, der Rest des Vertrags bleibt grundsätzlich unberührt. Im Falle eines Missbrauchs dürfen die Daten von keiner der beiden Vertragsparteien genutzt werden. Diese Regelungen sollen auch für künftiges sektorielles Datenzugangsrecht gelten. Sie sind auch auf Verträge anwendbar, bei denen auf beiden Seiten KMU stehen.

3.2.2 Bewertung

Im Rahmen der Missbrauchskontrolle soll keine Gesamtbewertung des Vertrags stattfinden. Das kann allerdings insofern problematisch werden, als Daten – wie mittlerweile auch im europäischen Recht klargestellt – Gegenleistung sein können. In diesen Fällen wird man immer im Sinne von Art. 13 Abs. 6 davon ausgehen müssen, dass die Klausel nicht vom Rest des Vertrags abtrennbar ist.

Es sollte klargestellt werden, dass Klauseln aus Musterverträgen der KOM (Art. 35) generell nicht der Missbrauchskontrolle unterliegen, auch dann nicht, wenn sie im Sinne von Art. 13 einseitig auferlegt wurden.

Obwohl in der Tradition klassischer Verbraucherschutzregelungen angelegt, greift der Entwurf weit in die unternehmerische Freiheit ein, insbesondere auch im Verhältnis B2B. Der Anwendungsbereich muss im Verhältnis zwischen Unternehmen zumindest deutlich eingeschränkt werden. Im weiteren Gesetzgebungsverfahren ist zu prüfen, wie diese überschießenden Regelungen zurückgefahren werden können. Denkbar wäre beispielsweise, die Missbrauchskontrolle auf von „Gatekeepern“ verwendete Klauseln zu beschränken, wo die Ungleichheit der Verhandlungsposition am höchsten sein dürfte. Die Größe des Unternehmens ist für sich betrachtet kein geeignetes Differenzierungskriterium, da eine starke Marktposition bei digitalen Anwendungen nicht notwendigerweise mit einer hohen Beschäftigtenzahl korreliert.

3.3 Datenbereitstellung für öffentliche Stellen und Forschung

3.3.1 Kerninhalt der Regelung

Vorgesehen ist in Kapitel 5 der Verordnung ein Datenzugang unter bestimmten Voraussetzungen für öffentliche Stellen (B2G). Sofern die Daten für die Bewältigung eines öffentlichen Notstands erforderlich sind, sollen sie kostenlos zur Verfügung gestellt werden, in den anderen Fällen einer „außergewöhnlichen Notwendigkeit der Datennutzung“ erfolgt die Bereitstellung gegen eine Gebühr, in die auch ein Gewinn für das Unternehmen einkalkuliert sein kann. Die staatlichen Stellen sind berechtigt, die von ihnen bei Unternehmen erhobenen Daten Forschungseinrichtungen und statistischen Ämtern zugänglich zu machen. Sonstige Informationsanforderungen, Berichtspflichten und so weiter bleiben unberührt, von denen es bereits zahlreiche gibt.

3.3.2 Bewertung

Grundsätzlich wäre es sehr wünschenswert, wenn der Staat künftig auf Basis aktueller und qualitativ hochwertiger Daten seine Entscheidungsgrundlagen insbesondere in Krisensituationen verbessern könnte. Das Haupthindernis liegt allerdings nicht in einer fehlenden Bereitschaft der Unternehmen, Daten zu teilen, sondern in der nach wie vor unzureichenden Digitalisierung der Verwaltung.

Die Anforderungen an ein wirksames Datenbereitstellungsverlangen sind durchaus hoch – was man sich in anderen Bereichen auch wünschen würde – aber umso mehr fragt sich, welchen praktischen Nutzen die Regelung entfalten kann. Unternehmen haben immer wieder eine große Bereitschaft gezeigt, Informationen mit öffentlichen Stellen zu teilen, erst recht in Krisensituationen. Mit der vorgeschlagenen Neuregelung würden sich die Möglichkeiten für staatliche Stellen nicht nennenswert verbessern, zumal hier auch nur

von „Daten“ (also nach unserem Verständnis Rohdaten) die Rede ist, und kritisch hinterfragt werden kann, wer diese dann tatsächlich schnell nutzen könnte. Das dürfte regelmäßig allenfalls bei den Forschungseinrichtungen und statistischen Ämtern der Fall sein. Diese profitieren aber auch kaum von der Regelung, weil sie nur ein abgeleitetes Zugangsrecht bekämen und auch das nur in den in Art. 15 definierten Fällen einer außergewöhnlichen Notwendigkeit. Zusätzlich gelten auch hier die bereits angesprochenen Probleme etwa im Hinblick auf das Datenschutzrecht und den Schutz von geistigem Eigentum, zumal die Zugangspflichten relativ weit reichen.

Ein Regelungsbedarf ist nicht ersichtlich. Im Kontext Datenwirtschaft wäre es wesentlich wichtiger, endlich die von der öffentlichen Hand mit Steuergeldern erhobenen Daten umfänglich zur Verfügung gestellt werden (Open Government Data), gegebenenfalls auch Regelungen für ein besseres Zusammenspiel von Wirtschaft und Wissenschaft im Hinblick auf den Umgang mit Daten zu entwickeln.

4 Weitere Regelungsinhalte

Flankierende und weiterführende Inhalte stehen teilweise etwas zusammenhanglos im Gesetz

4.1 Wechsel zwischen Datenverarbeitungsdiensten

4.1.1 Kerninhalt der Regelung

Der Wechsel zwischen verschiedenen Anbietern – insbesondere Cloud-Anbietern – soll erleichtert werden. Dabei soll es dem Kunden ermöglicht werden, alle seine digitalen Vermögenswerte einschließlich Daten und von ihm erzeugte Metadaten zu übertragen und deren Nutzung in der neuen Umgebung unter Aufrechterhaltung der Funktionsäquivalenz fortzusetzen. Zu den Vermögenswerten soll alle digitalen Elemente zählen, an denen der Kunde ein Nutzungsrecht hat, etwa Anwendungen oder virtuelle Maschinen. Der Cloud-Anbieter muss dabei jede erforderliche Unterstützung leisten, ist aber nicht verpflichtet, neue Kategorien von Diensten zu entwickeln, um Funktionsäquivalenz zu gewährleisten. Damit werden die Portabilitätsregelungen der DSGVO ergänzt.

4.1.2 Bewertung

Die Bedeutung von Cloud-Anwendungen für die Unternehmen steigt stetig. Es ist daher richtig, Lock-in-Effekte zu reduzieren und Wechselmöglichkeiten zu eröffnen. Nicht nachvollziehbar ist dagegen, in welchem Verhältnis das Kapitel VI des Entwurfs zu den sonstigen Regelungen steht. Schließlich werden auch die in den vorderen Kapiteln verpflichteten Dateninhaber und die Datenempfänger vielfach auf Cloud-Lösungen zurückgreifen.

4.2 Schutzvorkehrungen für nicht personenbezogene Daten im internationalen Umfeld

4.2.1 Kerninhalt der Regelung

Anbieter von Datenverarbeitungsdiensten müssen Schutzvorkehrungen treffen, um den unrechtmäßigen Zugang Dritter zu nicht personenbezogenen Daten zu verhindern, wenn diese nach Unionsrecht zu schützen sind. Staatliche Stellen von Drittländern sollen nur im Rahmen internationaler Vereinbarungen auf die Daten zugreifen können. Das Datenschutzrecht bleibt unberührt.

4.2.2 Bewertung

Lediglich aus den Erwägungsgründen lässt sich erschließen, an welche Konstellationen der Verordnungsgeber hier denkt, etwa an den Schutz von Geschäftsgeheimnissen. Das ist grundsätzlich zu begrüßen, allerdings wird der schon vorher durch die neuen Zugangsregelungen unterlaufen. Immerhin werden dann die davon noch nicht betroffenen Daten etwas besser geschützt.

4.3 Interoperabilität

4.3.1 Kerninhalt der Regelung

Kapitel VIII definiert Grundsätze, die von Betreibern von Datenräumen beachtet werden müssen und an denen sich Interoperabilitätsspezifikationen und europäische Normen für Datenverarbeitungsdienste orientieren müssen. Zusätzlich werden wesentliche Anforderungen an intelligente Verträge (Smart Contracts) für die gemeinsame Datennutzung festgelegt.

4.3.2 Bewertung

Entscheidend ist, dass Standardisierungsprozesse weiterhin bottom-up und praxisgetrieben erfolgen. Wo sich noch keine solchen Standards herausgebildet haben, ist das kein Zeichen dafür – wie die Kommission aber offenbar annimmt – dass Selbstregulierung nicht funktioniert hätte. Manche Entwicklungen stehen schlicht noch relativ am Anfang, was ihre praktische Bedeutung angeht. Bei Smart Contracts erkennt die KOM das indirekt ja sogar an, wenn sie in diesem Bereich nun zuerst auf ein Pilotprojekt setzt und sich im Rahmen des Data Acts auf Regelungen zu einzelnen technischen Aspekten beschränkt. Ein Regelungsbedarf ist aber auch hier sehr fraglich, weil der Einsatz eines Smart Contracts Beleg genug dafür ist, dass ein Wille zur Kooperation besteht.

4.4 Anwendung und Durchsetzung

Interessant ist hier insbesondere die in Art. 34 vorgesehene Erstellung von unverbindlichen Mustervertragsbedingungen für den Datenzugang und die Datennutzung durch die Kommission. Musterverträge beziehungsweise Mustervertragsklauseln sind als Instrument sehr zu begrüßen. Das gilt selbstverständlich auch für den Bereich der DSGVO, wo es seit Jahren auf europäischer wie auf nationaler Ebene versäumt wurde, entsprechende Hilfestellungen zu leisten. Es stellt sich allerdings die Frage, ob das nicht für große Teile der mit dem Data Act vorgeschlagenen verpflichtenden Regelungen von vornherein der bessere Weg wäre.

4.5 Ausnahme vom Datenbankschutzrecht

4.5.1 Kerninhalt der Regelung

Das spezifische Schutzrecht für die Inhalte von Datenbanken soll nach Art. 35 keine Anwendung auf Datenbanken finden, die Daten enthalten, die bei der Nutzung eines Produkts oder verbundenen Dienstes erlangt oder erzeugt wurden, um die Ausübung der Rechte nach Art. 4 und Art. 5 nicht zu behindern.

4.5.2 Bewertung

Die Formulierung ist jedenfalls viel zu weit und bedeutet damit einen unverhältnismäßigen Eingriff in den Datenbankschutz. Es darf nicht die Datenbank als solche ausgenommen werden, sondern allenfalls die konkreten Daten, für die ein Zugangsanspruch geltend gemacht wird – und auch erst ab diesem Zeitpunkt und nur soweit es für die Erfüllung von Verpflichtungen nach dem Data Act notwendig ist. Die Extraktion eines (nicht wesentlichen) Teils ist grundsätzlich auch im Rahmen des bestehenden Sui-generis-Schutzes möglich.

4.6 Umsetzungszeitraum

Zum aktuellen Stand ist offen, ab wann die Regelungen in Kraft treten könnten und wie lang die Frist für die Umsetzung sein wird. Bliebe es bei den im Entwurf vorgesehenen Regelungen, dann wäre angesichts der umfangreichen notwendigen Anpassungen jedenfalls ein langer Übergangszeitraum erforderlich. Für bereits abgeschlossene Verträge und die in diesem Rahmen übertragenen Daten muss Bestandsschutz gelten; der Zugangsanspruch darf auch für den Nutzer nur ex nunc greifen.

Ansprechpartner / Impressum

Christine Völzow
Geschäftsführerin,
Leiterin der Abteilung Wirtschaftspolitik

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

Impressum

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

Herausgeber

vbw
Vereinigung der Bayerischen
Wirtschaft e. V.

Max-Joseph-Straße 5
80333 München

www.vbw-bayern.de