Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V.
Bundesverband deutscher Banken e. V.
Bundesverband Öffentlicher Banken Deutschlands e. V.
Deutscher Sparkassen- und Giroverband e. V.
Verband deutscher Pfandbriefbanken e. V.

Die Deutsche Kreditwirtschaft

Stellungnahme

zum Vorschlag für ein europäisches Datengesetz (Data Act)

Lobbyregister-Nr. R001459
EU-Transparenzregister-Nr. 52646912360-95

Kontakt:
Stephan Mietke
Director
Telefon: +49 30 1663-2325
E-Mail: stephan.mietke@bdb.de

Berlin, 12. Mai 2022

Federführer:
Bundesverband deutscher Banken e. V.
Burgstraße 28 | 10178 Berlin
Telefon: +49 30 1663-0
www.die-deutsche-kreditwirtschaft.de

Vorbemerkung

Wir begrüßen das mit dem Vorschlag für ein europäisches Datengesetz verfolgte Ziel, durch einen horizontalen Rechtsrahmen für den Datenzugang und -austausch für Verbraucher und Unternehmen sowie zwischen diesen zu fördern. Datengetriebenen Innovationen und Services werden zunehmend wichtiger, für einzelnen Unternehmen wie auch die europäische Volkswirtschaft insgesamt. Dies erfordert nicht nur Zugang zu Daten entlang der gesamten Wertschöpfungskette über die verschiedenen beteiligten Leistungserbringer; es bedarf auch dem Zugang zu Daten aus ganz unterschiedlichen Anwendungsbereichen und Branchenkontexten, um Kundenbedürfnisse besser zu verstehen und zu befriedigen.

Daher sollten Kunden generell in die Lage versetzt werden, Zugang zu den die von Ihnen bereitgestellten oder generierten Daten zu erhalten und diese auch mit Dritten teilen, und zwar über eine digitale Schnittstelle möglichst in Echtzeit, damit die Daten nahtlos in Geschäftsprozesse integriert und somit unmittelbare Kundenmehrwerte beim Unternehmen oder Verbrauchers generiert werden können.

Insofern unterstützen wir zwar die im Datengesetz vorgesehenen neuen Verpflichtungen für den Zugang zu Daten aus vernetzten Produkten und damit verbundenen Diensten, die Kunden durch die Nutzung der Produkte und Services erzeugen. Die Begrenzung des Anwendungsbereiches auf maschinengenerierte Daten greift unseres Erachtens allerdings zu kurz, da viele Daten hiervon nicht erfasst wären und somit wesentliche Potenziale für neue und verbesserte Produkte und Dienstleistungen unter anderem im Banking ungenutzt blieben. Dies betrifft beispielsweise Nutzerdaten im Telekommunikationsbereich, der Energieversorgung oder dem Online-Handel, die nach unserem Verständnis nicht in den Anwendungsbereich fallen würden, sofern sie nicht über vernetzte Produkte erzeugt werden, gleichzeitig aber branchenübergreifend viele Anwendungsfälle ermöglichen könnten und eine größere sektorübergreifende Wiederverwendung von Daten insgesamt befördern würden. Nicht zuletzt könnte eine breitere Verfügbarkeit von Nutzerdaten über den IoT-Kontext hinaus auch bei der Transformation hin zu einer Green Economy einen wichtigen Beitrag leisten könnten.

Ergänzende sektorale Regelungen für einzelne Europäische Datenräume, wie sie die EU-Kommission im Bereich der Finanzwirtschaft durch ein separates Rahmenwerk für ein offenes Finanzwesen (Open Finance Framework) angekündigt hat, liefen einer integrierten Datenökonomie angesichts sektorübergreifender Mehrwertpotenziale vieler Daten und zunehmend verschwimmender Branchengrenzen zuwider. Etwaige sektorale Regelungen dürfen diesen einheitlichen Rahmen allenfalls flankieren, z.B. im Bereich der Standardisierung, ohne abweichende oder überschießende Regelungen auch im Sinne eines Level-Playing-Field zu schaffen.

Vor dem Hintergrund der steigenden Marktdurchdringung und Diversifizierung von außereuropäischen Technologiekonzernen bzw. Plattformunternehmen unterstützen wir ausdrücklich, dass Gatekeeper-Plattformen im Sinne des Digital Market Act im Rahmen des Data Act nicht Datenempfänger sein können. Dies trägt zum Abbau bestehender Marktasymmetrien bei.

Der Gesetzesvorschlag beschränkt sich allerdings auf Regelungen zu einem obligatorischen Datenzugang und lässt Regelungen zur Datenbereitstellung und -nutzung auf freiwilliger Basis vermissen, die als Grundlage für das Entstehens europäischer Datenräumen wünschenswert wären.

Im Übrigen muss sichergestellt werden, dass eine Erfüllung der Pflichten aus dem Data Act nicht im Konflikt zu anderen gesetzlichen bzw. rechtlichen Anforderungen steht oder zu einem Verstoß gegen vertragliche Verpflichtungen führt.

Datenaustausch B2C und B2B (Kapitel II)

Wir unterstützen die im Gesetzesvorschlag in den Artikeln 3 bis 6 enthaltenen Regelungen nach einem neuen Datenzugangs- und -teilungsrecht für die durch von Verbrauchern und Unternehmen generierten Daten im Sinne der Erhöhung der Datensouveränität und der Verfügbarmachung von Daten für die Nutzung durch Dritte.

Banken können demgemäß als Drittpartei auftreten, die auf Wunsch des Nutzers die durch ihn erzeugten Daten empfängt und auswertet. Auf diese Weise können Banken ihren Kunden neue oder verbesserte Dienstleistungen z.B. im Bereich der Kreditvergabe oder im Zahlungsverkehr anbieten, die sich auf Nutzungsdaten stützen. Damit Banken diese Rolle gemäß dem Wunsch ihrer Kunden auch in Zukunft einnehmen können, sollte die Möglichkeiten des Empfangs und der Auswertung dieser Daten möglichst nicht eingeschränkt werden.

Obwohl der Data Act den Anspruch einer sektorübergreifenden Regulierung hat, sind ausschließlich Hersteller und Nutzer von vernetzten physischen Produkten betroffen (sowie Drittparteien als Datenempfänger), was den Anwendungsbereich stark einschränkt.

Darüber hinaus können auch wettbewerbssensible Daten Gegenstand des Rechts auf Datenzugang und -weitergabe sein. Die Weitergabe von Daten, die Rückschlüsse auf ein bestimmtes Wettbewerbsverhalten zulassen (z. B. Preisinformationen, kundenspezifische Informationen, Verkaufszahlen, Kapazitäten, Entwicklungen, strategische Planung), ist aufgrund von Art. 101 AEUV untersagt. Infolgedessen kann es in der Praxis für Dateninhaber und Datenempfänger erhebliche Schwierigkeiten geben, zu bestimmen, welche Daten rechtmäßig weitergegeben werden können, ohne gegen das Wettbewerbsrecht zu verstoßen.

Verpflichtungen für Dateninhaber (Kapitel III)

Wir begrüßen die in Artikel 8 vorgesehene Vorkehrung, dass die Bedingungen für den Datenzugang zwischen Dateninhaber und Datenempfänger vereinbart werden sollen einschließlich der Maßgabe, dass diese fair, angemessen und diskriminierungsfrei sein müssen. Insbesondere die in Artikel 9 vorgesehene Möglichkeit des Dateninhabers, von dem Datenempfänger eine angemessene Gegenleistung für die Verfügbarmachung der Daten verlangen zu können, trägt dem Bedarf nach einem fairen Interessenausgleich zwischen den beteiligten Parteien unter Berücksichtigung von Kosten und Nutzen Rechnung.

Allerdings halten wir die in Artikel 9 Absatz 3 vorgenommenen Ausnahmen, das durch anderes Unionsrecht eine Gegenleistung eingeschränkt werden kann, für zu weitgehend und mit den Zielen des Data Act zur Etablierung eines konsistenten horizontalen Rechtsrahmen nicht vereinbar.

Die Möglichkeit des Dateninhabers, eine angemessene Gegenleistung für die Bereitstellung von Daten zur erhalten ist eine Thematik, die im Zahlungsdienstebereich beim Zugriff von Drittanbietern auf Zahlungskontodaten ausgeschlossen ist: Banken stellen Drittanbietern im Rahmen der Anforderungen der zweiten Zahlungsdiensterichtlinie (PSD2) seit langem Kontodaten über standardisierte Schnittstellen zur Verfügung, deren Aufbau und Betrieb mit signifikanten Kosten verbunden sind, für die jedoch kein Entgelt erhoben werden darf. Es wäre wünschenswert, dass eine Kompensation für den Datenzugang im Zusammenhang mit diesen Diensten ermöglicht wird und die damit entstandenen Ungleichgewichte im Rahmen einer Überarbeitung der Zahlungsdiensterichtlinie korrigiert werden. Der europäische Gesetzgeber sollte eine Vergütung für den Datentransfer im Bankensektor weder pauschal verbieten, noch anordnen, sondern den Marktteilnehmern adäquate Lösungen ermöglichen.

Darüber hinaus bedarf es einer Klarstellung, auf welche Datenbereitstellungpflichten sich die Regelungen in Kapitel III beziehen. Es ist nicht eindeutig ersichtlich, ob sich diese nur auf den Datenaustausch zwischen privaten Parteien als Dateninhaber bzw. Datenempfänger beziehen oder auch auf den Austausch mit dem öffentlichen Sektor. So wäre auch im Zusammenhang mit den Datenbereitstellungspflichten gegenüber öffentlichen Stellen nach Kapitel V dieser Vorordnung ein Streitbeilegungs-Mechanismus wünschenswert.

Bereitstellung von Daten an den öffentlichen Sektor (B2G) (Kapitel V)

Wir teilen grundsätzlich das Bestreben, den öffentlichen Sektor in die Lage zu versetzen, Entscheidungen auf Grundlage einer solider Datenbasis zu treffen und von der steigenden Datenverfügbarkeit im Digitalzeitalter zu partizipieren. Der öffentliche Sektor verfügt allerdings bereits über umfangreiche Datenbestände, die es hierfür vorrangig und wirksam zu nutzen gilt. Ein zusätzlicher Zugriff auf privatwirtschaftliche Daten sollte nur dort erwogen werden, wo es unvermeidbar ist, insbesondere in außergewöhnlichen Notlagen.

Im Hinblick auf die in den Artikeln 14 ff. vorgesehenen Regelungen zur Bereitstellung von Daten an den öffentlichen Sektor haben wir die Sorge, dass es zu einer übermäßigen Inanspruchnahme und zu hohem Aufwand bei den betroffenen Unternehmen führen könnte, zumal die Verpflichtung ohne erkennbare Einschränkung unmittelbar gegenüber jedweder öffentlichen Stelle gilt. Aus unserer Sicht fehlt es unter anderem an einem ex-ante Kontrollmechanismus, über den die Verhältnismäßigkeit der Datenzugangsanfragen sichergestellt wird. Liegt die Entscheidung allein bei der öffentlichen Stelle, die die Daten selbst anfordert und ein Interesse an der Erhebung hat, fehlt es an der gebotenen Unabhängigkeit. Zudem ist völlig unklar, nach welchen Kriterien Unternehmen ausgewählt werden, die die Daten bereitstellen sollen. Dies

lässt Freiraum für willkürliche Entscheidungen und kann zur Benachteiligung einzelnen Marktteilnehmer führen.

Ferner ist nicht erkennbar, wie einem potenziellen Missbrauch oder der Verletzung sensibler Daten wirksam vorgebeugt werden soll und wie Betroffene gegebenenfalls Regressansprüche geltend machen können. Die Verpflichtung der datenempfangenden öffentlichen Institutionen nach Artikel 19, Maßnahmen zu treffen, um die Datenschutzrechte der Betroffenen und den Schutz von Geschäftsgeheimnissen und geistigem Eigentum zu wahren, ist unseres Erachtens nicht ausreichend und höhlt rechtsstaatliche Grundsätze aus. Problematisch bewerten wir auch die Regelung in Artikel 21, wonach öffentliche Institutionen die Daten für wissenschaftliche oder andere Analysezwecke ohne Zustimmung der Betroffenen an Dritte weitergeben können. Der Dateninhaber sollte steuern können, ob seine Daten an Dritte weitergeben werden, wenn diese nicht vor Weitergabe anonymisiert worden sind.

Der Data Act darf nicht im Konflikt mit anderen EU-weiten oder nationalen Gesetzen oder regulatorischen Anforderungen, wie z.B. der EU-DSGVO oder einschlägiger nationaler Regulatorik, sowie vertraglich festgehaltenen Vereinbarungen stehen. Es sollte klar definiert werden, wie der Data Act mit anderen Rechtsakten zusammenspielt und welches Gesetz Vorrang hat.

Weiterhin müssen angemessene Informationssicherheitsmaßnahmen eingehalten werden, wenn ein Unternehmen Daten an andere Organisationen weitergibt. Dies wird nicht nur von einschlägigen regulatorischen Anforderungen gefordert, sondern ist auch für ein Unternehmen essenziell. Daten müssen gemäß ihres Schutzbedarfes gesichert werden, unabhängig davon an wen sie weitergegeben werden.

Darüber hinaus gibt es viele Bereiche, in denen Behörden bereits umfassende Rechte auf Zugang zu verschiedenen Daten haben, um die ihnen übertragenen Aufgaben zu erfüllen. Dies gilt insbesondere für Aufsichtsbehörden im Finanzsektor zum Zwecke der Sicherung der Finanzstabilität. Es sollte klargestellt werden, dass in diesen Fällen, in denen bereits Rechtsgrundlagen bestehen, die Bestimmungen dieser Verordnung keine Anwendung finden sollen.

Wechsel zwischen Datenverarbeitungsdiensten (Kapitel VI)

Die vorgesehenen Regelungen zur Beseitigung von Hindernissen für einen effektiven Wechsel zwischen Anbietern von Datenverarbeitungsdiensten bewerten wir grundsätzlich positiv. Sie helfen, Marktasymmetrien abzubauen und Vendor-Lock-Ins aufzubrechen, indem sie die Rechte der Kunden von Datenverarbeitungsdiensten in einem stark konzentrierten Markt stärken.

Dabei muss der Eingriff in den Markt allerdings wohl dosiert sein, um zu verhindern, dass sich Anbieter von Datenverarbeitungsdiensten ganz aus diesem zurückziehen bzw. Hürden für den Markteintritt neue Anbieter entstehen, die zu einer Reduzierung des Angebotes und damit zum gegenteiligen Effekt des eigentlichen Ansinnens nämlich einer Eindämmung des Wettbewerbs führen könnten.

Eine vollständige Portabilität der Funktionalitäten von Datenverarbeitungsdiensten halten wir weder für erstrebenswert noch für realisierbar, insbesondere je komplexer die Anwendungen werden. Denn es würde Marktinnovationen und die Nutzung zukünftiger Technologien verhindern.

Der vorgesehene Zeitraum von maximal 30 Tagen für den Datentransfer von einem zum anderen Dienstleister erscheint im Kontext der üblichen Komplexität und der regulatorischen Anforderungen an Datenverarbeitungsdienste in der Finanzbranche deutlich zu kurz und in der Praxis nicht umsetzbar. Deshalb sprechen wir uns dafür aus, dass auch längere Zeiträume vertraglich vereinbart werden können.

Zudem bedarf es einer Klarstellung, wer als Anbieter von Datenverarbeitungsdiensten von den Artikeln 23 ff. betroffen wäre. Artikel 2 Absatz 12 definiert den Begriff des "Datenverarbeitungsdienstes" sehr weitreichend. In den Fällen, in denen Kapitel VI darauf abzielt, den Wechsel zwischen hauptsächlich Cloud- und Edge-Diensten zu erleichtern (siehe Erwägungsgrund 69), sind klare rechtliche Definitionen erforderlich. Denn heutzutage ist die Datenverarbeitung – in unterschiedlichem Ausmaß – Teil vieler Geschäftsvorgänge in verschiedenen Einrichtungen und nicht unbedingt nur auf Cloud- und Edge-Diensteanbieter beschränkt.

Interoperabilität (Kapitel VIII)

Für Privatpersonen und Unternehmen ist die Verbesserung der Interoperabilität ein wichtiger Faktor. Sie verringert die Abhängigkeit von einem Anbieter und erleichtert den Wechsel zu einem anderen Anbieter oder die Durchführung eines Ausstiegsszenarios. Interoperabilität trägt dafür Sorge, dass die Dienste ohne Beeinträchtigung der Funktionalität, Integrität und Verfügbarkeit problemlos zwischen verschiedenen Anbietern gewechselt werden können.

Um eine Interoperabilität zu gewährleisten, müssen einheitliche Standards zu Datenformaten und Schnittstellen entwickelt oder festgelegt werden. Wie und von wem diese Standards entwickelt werden, muss über die Anforderungen in Artikel 28 und 29 hinaus geklärt werden. Grundsätzlich befürworten wir eine marktgetriebene Entwicklung dieser Standards (self-regulation), da diese den Bedürfnissen der Stakeholder am besten gerecht wird.

Standardisierungsprozesse müssen jedoch transparent sein und die Beteiligung aller relevanten Interessengruppen ermöglichen. Auch sollten internationale Standards/Standardisierungs-gremien bei der Entwicklung berücksichtigt werden. Delegierte Rechtsakte, die Rahmenbedingungen für die Interoperabilität festlegen, halten wir für sinnvoll. Allerdings sollten diese im Einklang mit existierenden regulatorischen und aufsichtsrechtlichen Anforderungen an die Finanzbranche sein.

Zudem stellt Artikel 28 konkrete Interoperabilitätsanforderungen an Betreiber von Datenräumen. Mangels einer Definition des Begriffs „Datenraum" ist allerdings unklar, was genau unter diesem Konzept zu verstehen ist und wer als Betreiber zu betrachten wäre. Hierzu ist eine Klarstellung erforderlich.

Mit Blick auf Smart Contacts messen wir diesen hohes Potenzial bei, Austauschbeziehungen von Gütern oder Dienstleistungen im Kontext vernetzter Produkte (Internet of Things) und auch darüber hinaus zwischen einzelnen Vertragsparteien zu vereinbaren und automatisiert abzuwickeln. Smart Contracts ausschließlich im Kontext einer gemeinsamen Datennutzung zu regeln, wie im Verordnungsvorschlag unter Artikel 30 vorgesehen, greift allerdings zu kurz. Hierzu folgendes Beispiel: Ein Unternehmen finanziert seinen vernetzten Maschinenpark nutzungsabhängig, d.h. abhängig von der tatsächlichen Nutzungsintensität der einzelnen Maschine wird die jeweilige zu entrichtende Finanzierungsrate an die finanzierende Bank berechnet. Über einen Smart Contract könnten die Nutzungsdaten stichtagsbezogen der Bank zugänglich gemacht werden, z.B. indem sie in der Blockchain (verschlüsselt) abgelegt werden. Der Maschinennutzung steht jedoch ein Entgeltanspruch in Form einer Leasing- oder Kreditrate der finanzierenden Bank gegenüber, der idealerweise ebenfalls Gegenstand des Smart Contracts ist. In diesem Falle würde der Smart Contract nicht nur die gemeinsame Datennutzung (als Berechnungsgrundlage für die Kredit-/Leasingrate) umfassen, sondern gleichzeitig eine Zahlung vom Unternehmen an die Bank, idealerweise vollständig automatisiert, auslösen. Letzteres wird jedoch erschwert durch das geltende Zahlungsrecht (PSD2), das als Grundannahme die (manuelle) Autorisierung einer Zahlung des Zahlers und dessen Authentifizierung durch Bank trifft und somit für vollautomatisierte Zahlungsaufträge rechtliche Unsicherheiten und Komplexitäten impliziert. Diese Herausforderung resultiert insbesondere aus den allgemeinen zivilrechtlichen Grundsätzen, wonach Aufträge immer von einem Menschen erteilt werden müssen.

An diesem Beispiel wir deutlich, dass es einer umfassenderen Regelungen der Rahmenbedingungen für Smart Contracts bedarf, die über den aktuellen, datenbezogenen Regelungsumfang der Verordnung deutlich hinaus gehen. Vereinzelte Regelungen in unterschiedlichen Anwendungsbereichen bergen die Gefahr eines inkonsistenten Rechtsrahmens, der einer wirtschaftlichen Verbreitung von Smart Contracts im Wege steht. Eine ganzheitliche Betrachtung von Smart Contracts im Sinne von Art. 2 Nr. 16 durch den Gesetzgeber im Lichte weiterer einschlägiger Rechtsnormen und ihrer Eignung ist daher geboten.

Sonstiges

Im Übrigen begrüßen wir die in Artikel 27 (Kapitel VII) verankerten Vorkehrungen zum Schutz der Daten vor Zugriffen von Regierungen aus Drittstaaten, die Anbieter von Datenverarbeitungsdiensten zu treffen haben.