

STELLUNGNAHME

Stand: 18. Mai 2022

Vorschlag der Europäischen Kommission für eine Verordnung
des Europäischen Parlaments und des Rates über
harmonisierte Vorschriften für einen fairen Datenzugang und
eine faire Datennutzung (Datengesetz)

COM(2022) 68 final 2022/0047 (COD)

ZIA Zentraler Immobilien Ausschuss e.V.

Inhaltsverzeichnis

A.	Zusammenfassung	3
B.	Anmerkungen zum Vorschlag für eine Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz)	4
1)	Kapitel 1: Allgemeine Bestimmungen	4
2)	Kapitel 2: Datenweitergabe von Unternehmen an Verbraucher und zwischen Unternehmen	5
3)	Kapitel 3: Pflichten der Dateninhaber, die rechtlich verpflichtet sind, Daten bereitzustellen	6
4)	Kapitel 5: Bereitstellung von Daten für öffentliche Stellen und Organe, Einrichtungen und sonstige Stellen der Union wegen außergewöhnlicher Notwendigkeit	6
5)	Kapitel 6: Wechsel zwischen Datenverarbeitungsdiensten	7
6)	Kapitel 7: Schutzvorkehrungen für nicht personenbezogene Daten im internationalen Umfeld	7
7)	Kapitel 8: Interoperabilität	7

A. Zusammenfassung

Der ZIA befürwortet, dass die Potenziale von Daten stärker als bisher gehoben werden sollen. Gerade auch im Hinblick auf Klima- und Umweltschutz kann etwa die Einführung digitaler Gebäudeinfrastruktur für Verbrauchsmessungen bei der Reduzierung von CO₂-Emissionen helfen. Ob „Smart Metering“, intelligente Lichtsysteme, vernetzte Videokameras oder Bewegungsmelder – die Immobilienwirtschaft verwaltet große Mengen an personenbezogenen Daten. Der Datengesetz-Entwurf hat dabei das Potenzial, Rechtsunsicherheiten beim Umgang mit personenbezogenen und nicht-personenbezogenen Daten im Gebäudesektor abzubauen und kann notwendige Rahmenbedingungen schaffen, dass etwa Gebäudeeigentümer und (auftragsverwaltende) Dienstleister die benötigten Daten erhalten können.

Insgesamt begrüßt der ZIA daher die Schaffung eines Rahmenwerks für die europäische Datenwirtschaft. Insbesondere werden damit Grundlagen für die Schaffung gemeinsamer Europäischer Datenräume gelegt. Die Entwicklung von Standards ermöglicht eine (sektorübergreifende) Interoperabilität. Ein Aufbrechen von Markt-Asymmetrien gegenüber großen Konzernen durch die Stärkung von Kleinen Unternehmen und Start-ups / PropTechs, Kunden von Cloud-Diensten und Privatpersonen wird ermöglicht. Zugriffsrechte und Datenhoheit werden definiert, Missbrauch vermieden und mehr Transparenz bei der Nutzung von Daten geschaffen. Dies umfasst auch den Schutz vor illegaler Datenübermittlung in Drittländer und Zugriff von Regierungen aus Drittstaaten. Schließlich wird damit auch die Entwicklung neuer Geschäftsmodelle mit maschinengenerierten Daten gefördert.

Zur Abgrenzung zwischen personenbezogenen und nicht personenbezogenen Daten sollten Widersprüche zwischen DSGVO und Datengesetz-Entwurf zwingend aufgelöst werden. Der Mehraufwand etwa bei der Bereitstellung von Daten In Echtzeit sollte minimiert werden. Kontrolle, Nachweis und Durchsetzung von Nutzungsbeschränkungen für Weiterverwender sollten präzisiert werden. Ebenso bedarf es eines Kontrollmechanismus gegenüber der öffentlichen Institution, um zu prüfen, ob das Datenverlangen gerechtfertigt ist. Bei der Bereitstellung von Daten in einem B2G-Kontext haben öffentliche Institutionen deutlich zu viele Rechte – Unternehmen können eine Anfrage bei erhöhter Vertraulichkeitsstufe nicht ablehnen. Das Prinzip der freien Marktwirtschaft und zentrale rechtsstaatliche Grundsätze werden ausgehebelt, da öffentliche Institutionen Zugriff auf personenbezogene Daten einfordern können, ebenso eine Weitergabe von Geschäftsgeheimnissen. Ein Überwachungsmechanismus wäre auch für die Forschungseinrichtungen nötig, an denen die Daten weitergegeben werden können.

Nachfolgend nehmen wir zu den einzelnen Aspekten des Verordnungsvorschlags Stellung.

B. Anmerkungen zum Vorschlag für eine Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz)

1) Kapitel 1: Allgemeine Bestimmungen

Zur Abgrenzung zwischen personenbezogenen und nicht personenbezogenen Daten sollten Widersprüche zwischen DSGVO und Datengesetz-Entwurf zwingend aufgelöst werden. Im Datengesetz-Entwurf sollten Regelungen getroffen werden, die einen zulässigen Datentransfer definieren, reglementieren und dabei nicht im Widerspruch zu DSGVO stehen. So sollte sichergestellt sein, dass die personenbezogenen Daten Dritter, nicht Unbefugten zugänglich gemacht werden dürfen. Dies ist insbesondere auch dann zu beachten, wenn die ursprünglichen Daten aufgrund einer Einwilligung gem. Art. 6 Abs. 1 lit. a DSGVO erhoben wurden, welche jederzeit widerrufbar wäre und von einer späteren Datenübermittlung ursprünglich nicht ausgegangen werden konnte bzw. bei einem Widerruf dann von allen Datenempfängern/Nutzern auch entsprechend umgehend gelöscht werden müssten.

Um Unklarheiten vorzubeugen, sollte in der deutschen Fassung vom „Datenhalter“ (wie im Englischen) anstelle vom „Dateninhaber“ gesprochen werden. Ein „Dateninhaber“ wäre im Sinne der DSGVO wohl mit dem „Verantwortlichen“ und/oder „der betroffenen Person“ gleichzusetzen, d.h. dem die personenbezogenen Daten gehören, oder in dessen Auftrag diese verarbeitet werden. Dies ist aber nicht mit dem Dienstbringer gleichzusetzen, da dieser hier auch im Auftrag des Verantwortlichen diese Daten als „Auftragsverarbeiter“ im Sinne der DSGVO verarbeiten kann und dann weisungsgebunden gegenüber dem „Dateninhaber“ wäre. Das kann insbesondere im Kontext von Verträgen zur Auftragsverarbeitung im Sinne Art. 28 DSGVO dann zu Kollisionen in den Begrifflichkeiten führen, da hier der „Dateninhaber“ immer der weisungsbefugte Auftraggeber ist, der auch über die Gestaltung der Dienste bestimmen kann.

Klargestellt werden sollte dabei auch, ob der „Dateninhaber“ derjenige ist, der das Produkt herstellt oder vielmehr derjenige, der die Kontrolle über die Daten hält.

Die Definition von „Daten“ sollte präziser gefasst werden, vor allem im Hinblick auf die Schwelle zu den „aus diesen Daten abgeleitete[n] oder gefolgerte[n] Informationen“ (Erwägungsgrund 14). Es muss klar bestimmt sein, ob lediglich Rohdaten erfasst sind (und wann Rohdaten durch Analyse und Verarbeitung zu abgeleiteten und gefolgerten Informationen werden), ob lediglich vom „Dateninhaber“ tatsächlich für seine eigenen Geschäftsvorfälle verwendete Daten betroffen und keine flüchtigen Daten von der Definition umfasst sind. Zudem muss sichergestellt werden, dass sich keinerlei (Gewährleistungs- bzw. Haftungs-)Ansprüche aufgrund ihrer Beschaffenheit ergeben.

Um Rechtssicherheit zu gewährleisten, sollte klargestellt werden, dass es mehrere „Nutzer“ geben kann, die ja auch juristische Personen sein können, etwa Mieter und Vermieter bei Heizungsabrechnungsdaten oder mehrere Eigentümer einer Immobilie.

Weiterhin sollten zur Vermeidung von Rechtsunsicherheit Anforderungen für eine datenschutzkonforme Anonymisierung personenbezogener Daten dargelegt werden.

2) Kapitel 2: Datenweitergabe von Unternehmen an Verbraucher und zwischen Unternehmen

Kapitel 2 regelt die Datenhoheit von und den Zugang zu maschinengenerierten Daten. Unternehmen wird damit auch neuer Zugang zu Daten gegeben. Dies fördert neue Business Cases / Use Cases mit maschinengenerierten Daten (datenbezogene Services), **bricht Asymmetrien im Markt auf und sorgt für eine bessere Verteilung von Daten unter Marktteilnehmern.**

Es kann eine erhöhte Transparenz von mieterbezogenen Nutzungsdaten am Markt entstehen, **wenn Mieter die Datenweitergabe an Dritte autorisieren – insbesondere Verbrauchsdaten** (bspw. zur Optimierung oder Ermittlung des ESG-Profiles eines Bestandshalters), **Gebäudenutzungsdaten** (bspw. IoT-Daten zur Optimierung des Flächenbedarfs) und **Daten über Mietkonditionen** (bspw. zum Mieten-Benchmarking gegenüber Wettbewerbern).

Allerdings besteht bereits ein anfänglicher Mehraufwand, da Nutzer die Bereitstellung von Daten erst autorisieren müssen. **Darüber hinaus entsteht weiterer Mehraufwand, da Daten in Echtzeit übertragen werden sollen und die Datensicherheit bei dem Nutzer und dem autorisierten Dritten sichergestellt werden muss. Der Nutzer und der autorisierte Dritte können jedoch nur schwer überwacht werden.**

Hinzu kommt, dass Art. 4 und 5 ggf. **den Vermieter dazu verpflichten, jedes generierte Datum zu speichern (unklar für welche Dauer).** Hierunter fielen auch temporäre Daten, die, gemäß ihrer Definition, in regelmäßigen Abständen überschrieben werden. Sollte es keine diesbezügliche Einschränkung geben, müssten große Mengen an nicht wiederverwertbaren Daten „on device“ oder in einer Cloud gespeichert werden. **Dies würde zu erheblichen administrativen Kosten, Energieaufwänden und Investitionen in die Datenhaltung führen.**

Ebenso unklar ist, wie Kontrolle, Nachweis und Durchsetzung von Nutzungsbeschränkungen für Weiterverwender (etwa das Verbot, die Daten für andere Zwecke oder für die Entwicklung von Konkurrenzprodukten zu nutzen) umgesetzt werden.

3) Kapitel 3: Pflichten der Dateninhaber, die rechtlich verpflichtet sind, Daten bereitzustellen

Kapitel 3 schafft ein Rahmenwerk für den Datenaustausch über Sektoren hinweg.

Es ist allerdings unklar, ob eine solcher Rahmen nötig ist, da Daten grundsätzlich nicht ohne vertragliche Basis weitergegeben werden können. Verträge mit Dienstleistern (bspw. Property Manager, Facility Manager etc.) müssen ergänzt werden um Regelungen zur Weitergabe von Nutzungsdaten (Verbrauchsdaten, Mietkonditionen etc.) an Dritte (Mieter, externe Dienstleister, öffentliche Hand). Hierbei sind auch kommerzielle Rahmenbedingungen abzustimmen. **Dies führt zu zusätzlichem Aufwand mit steigender Komplexität.**

Zudem ist der Begriff „angemessene Vergütung“ unkonkret.

4) Kapitel 5: Bereitstellung von Daten für öffentliche Stellen und Organe, Einrichtungen und sonstige Stellen der Union wegen außergewöhnlicher Notwendigkeit

Kapitel 5 zielt insbesondere auf Daten privatwirtschaftlicher Unternehmen, die am Markt nicht frei erworben werden können. **Objektbezogene Verbrauchs-/ESG-Daten könnten damit von öffentlicher Hand angefordert werden, um die Erreichung der Klimaziele besser steuern zu können. Auch würden so ein transparentes Benchmarking bzw. eine wirksame Steuerung entlang der EU-Taxonomie ermöglicht werden.**

Es handelt sich jedoch um eine übermäßige Inanspruchnahme der Daten von Unternehmen. **Dem Missbrauch oder der Verletzung sensibler Daten wird nicht hinreichend vorgebeugt, da (auch personenbezogene) Daten in sehr weit gefassten Situationen angefordert werden können. So ist unklar, wie mit Anfragen an Daten mit höchster Vertraulichkeitsstufe umzugehen ist.**

Auch ist es unklar, wie die Unternehmen ausgewählt werden, die die Daten bereitstellen sollen, und wer diese Unternehmen auswählt. **Es gibt keinen Kontrollmechanismus gegenüber der öffentlichen Institution um zu prüfen, ob der Anspruch gerechtfertigt ist.**

Die Weitergabe der Daten an Forschungseinrichtungen kann nicht verhindert werden. Es fehlt eine Überwachungsmechanismus der Forschungseinrichtungen, sodass unklar ist, was mit den Daten passiert. Die Unternehmen verlieren die Hoheit über die Daten und erhalten im Falle der Bewältigung eines öffentlichen Notstands keine Vergütung.

Schließlich sollte die Weitergabe von Daten an öffentliche Institutionen auch, wie in Kapitel 3, eine vertragliche Basis haben. Wichtig wäre einen Marktpreis für Daten aus dem professionellen Real Estate Umfeld zu definieren, um zu verhindern, dass

öffentliche Stellen – unabhängig von der Angemessenheit – exzessiven Gebrauch von Datennutzungsanfragen machen.

5) Kapitel 6: Wechsel zwischen Datenverarbeitungsdiensten

Kapitel 6 unterstützt die Rechte von Kunden von Cloud-Anbietern.

Es sollte konkret definiert werden, welche Dienstleistungen hierunter fallen.

Aus DSGVO-Sicht müsste zwingend ein Prüfprozess in Bezug auf personenbezogene Daten stattfinden unter Betrachtung eines zulässigen Erlaubnistatbestands gemäß Art. 6 Abs. 1 DSGVO, welcher einen Datenexport erlauben würde. Zudem könnte diese Regelung potenziell gravierende Auswirkungen für alle Vertragsparteien von Cloud- und Software-as-a-Service-Geschäftsmodelle haben. Ist es doch so, dass in der Regel weder der Nutzer diese Informationen verwerten kann, noch können diese Informationen in einer anderen Plattformumgebung (sinnvoll) genutzt oder technisch implementiert werden.

6) Kapitel 7: Schutzvorkehrungen für nicht personenbezogene Daten im internationalen Umfeld

Der erhöhte Schutz von nicht-personenbezogener Daten (Geschäftsgeheimnisse und das geistige Eigentum) in Kapitel 7 schafft mehr Vertrauen in Cloud-Dienste.

Es ist allerdings unklar, ob nicht-personenbezogene Daten grundsätzlich nicht in Drittländer übermittelt werden dürfen, die kein hinreichendes rechtliches Schutzniveau für Geschäftsgeheimnissen und geistigem Eigentum aus der EU bieten und in denen ebenfalls ein Risiko behördlicher Zugriffe besteht.

Ausnahmen geregelt sein, wenn internationale Abkommen mit der EU oder einzelnen Mitgliedsstaaten in Kraft sind und der Antrag des Drittstaates begründet, verhältnismäßig und spezifisch ist.

7) Kapitel 8: Interoperabilität

Die Förderung der Interoperabilität in Kapitel 8 legt einen Grundstein für gemeinsame Europäische Datenräume und wird für mehr Datennutzung und Datenaustausch sorgen. **Auch erhöht sich dadurch die Flexibilität beim Wechsel von Dienstleistern bzw. Versorgern, da Anspruch auf Bereitstellung relevanter Daten gegeben ist.**

Es sollte darauf geachtet werden, dass der Grundsatz der Technologieneutralität gewahrt wird und Innovationsanreize beibehalten werden. Normen und Spezifikationen müssen marktrelevant sein, d.h. in enger Abstimmung mit relevanten Wirtschaftsakteuren entwickelt werden.

Ansprechpartner

Daniel Bolder

Leiter Europabüro Brüssel

Tel.: +32 2 550 16 14

E-Mail: daniel.bolder@zia-deutschland.de

MEHR ZUM THEMA

EUROPA



Der Zentrale Immobilien Ausschuss e.V. (ZIA) ist der Spitzenverband der Immobilienwirtschaft. Er spricht durch seine Mitglieder, darunter 30 Verbände, für rund 37.000 Unternehmen der Branche entlang der gesamten Wertschöpfungskette. Der ZIA gibt der Immobilienwirtschaft in ihrer ganzen Vielfalt eine umfassende und einheitliche Interessenvertretung, die ihrer Bedeutung für die Volkswirtschaft entspricht. Als Unternehmer- und Verbändeverband verleiht er der gesamten Immobilienwirtschaft eine Stimme auf nationaler und europäischer Ebene – und im Bundesverband der deutschen Industrie (BDI). Präsident des Verbandes ist Dr. Andreas Mattner.

ZIA Zentraler Immobilien Ausschuss e.V.

Hauptstadtbüro

Leipziger Platz 9
10117 Berlin

Europabüro

3 rue du Luxembourg
B-1000 Brüssel



Telefon: +49 30 | 20 21 585 – 0

+32 | 2 5501614

E-Mail: info@zia-deutschland.de

Website: <https://zia-deutschland.de/>