Stellungnahme

der Clearingstelle des Landes Niedersachsen

zum

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

für

das Niedersächsische Ministerium für Wirtschaft, Arbeit, Verkehr und Digitalisierung

Hannover, den 20. April 2022

Inhaltsverzeichnis

I. Einleitung und Vorgehen der Clearingstelle des Landes Niedersachsen

Am 23. März 2022 wurde die **Clearingstelle des Landes Niedersachsen** (im Folgenden kurz „**Clearingstelle**“ genannt) per E-Mail vom **Niedersächsischen Ministerium für Wirtschaft, Arbeit, Verkehr und Digitalisierung** (im Folgenden kurz „**MW**“ genannt) mit der Anfertigung einer beratenden Stellungnahme zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz/Data Act) beauftragt. Das **MW** hat die **Clearingstelle** gebeten, bis zum 20. April 2022 eine Einschätzung abzugeben, ob der Vorschlag für ein Datengesetz und die darin vorgesehenen Mechanismen zur Ermöglichung von Datenaustausch für KMU umsetzbar und vor allem nutzbar sind und wies darauf hin, dass auch gern Vorschläge für bürokratieärmere Regelungen entgegengenommen werden würden, sofern diese benannt werden können.

Die **Clearingstelle** informierte ihrerseits am 24. März 2022 die Institutionen, die sich gemäß des Beiratsvertrags vom 14. Juli 2020 als Mittelstandsbeirat gemeinsam zur aktiven und konstruktiven Mitwirkung an Clearingverfahren und beratenden Stellungnahmen nach § 31a GGO sowie zur Unterstützung der **Clearingstelle** bei der Entwicklung alternativer bürokratievermeidender Regelungsvorschläge verpflichtet haben, über die Beauftragung und bat die Beiratsmitglieder unter Benennung weiterer Informationen zum geplanten Datengesetz um Übersendung ihrer Stellungnahmen bis zum 11. April 2022.

Neben dem **MW**, welches auch den Vorsitz des Mittelstandsbeirats übernommen hat, sind folgende Organisationen Mitglieder des Mittelstandsbeirats:

- Arbeitsgemeinschaft der kommunalen Spitzenverbände (**AG KSpV**),
- Verband der Freien Berufe im Lande Niedersachsen e.V. (**FBN**),
- IHK Niedersachsen – Landesarbeitsgemeinschaft der Industrie- und Handelskammern (**IHKN**),
- Landesvertretung der Handwerkskammern Niedersachsen (**LHN**),
- Landwirtschaftskammer Niedersachsen (**LWKN**),
- Unternehmensverbände Handwerk Niedersachsen e.V. (**UHN**) und
- Unternehmerverbände Niedersachsen e.V. (**UVN**).

Folgende Organisationen haben der **Clearingstelle** eine Stellungnahme zum Datengesetz zur Verfügung gestellt:

- **AG KSpV,**
- **IHKN,**
- **LHN,**

- **UHN** und
- **UVN**.

Die **Clearingstelle** hat die eingegangenen Stellungnahmen ausgewertet und gebündelt. Auf Grundlage der ihr vorliegenden Informationen sowie weiteren Recherchen hat die **Clearingstelle** für das **MW** die vorliegende beratende Stellungnahme mit Votum erstellt.

II. Hintergrund

Die EU-Kommission hat Ende Februar 2022 einen Vorschlag für ein Europäisches Datengesetz (Data Act) veröffentlicht. Mit diesem Gesetz soll der Zugang und Austausch von Daten für die Nutzung dieser zwischen Unternehmen (B2B), Unternehmen und Verbrauchern (B2C) und Unternehmen und Behörden (B2G) geregelt werden. Es soll dazu beitragen, „die Innovations- und Wettbewerbsfähigkeit, von EU-Unternehmen sämtlicher Branchen sicherzustellen, die Handlungskompetenz der Menschen in Bezug auf ihre Daten wirksam zu stärken und Unternehmen und öffentliche Stellen besser mit einem angemessenen und vorhersehbaren Mechanismus für die Bewältigung wichtiger politischer und gesellschaftlicher Herausforderungen, einschließlich öffentlicher Notstände und anderer Ausnahmesituationen, auszustatten.“[1].

Das Datengesetz soll dazu dienen, dass

- eine Erleichterung des Datenzugangs und der Datennutzung für Verbraucher und Unternehmen bei gleichzeitiger Aufrechterhaltung von Anreizen für Investitionen in die Wertschöpfung durch Daten erzielt wird,

- die Nutzung von im Besitz von Unternehmen befindlichen Daten durch öffentliche Stellen und Organe, Einrichtungen und sonstige Stellen der Union in bestimmten Situationen, in denen eine außerordentliche Notwendigkeit dazu besteht, ermöglicht wird,

- dass der Wechsel zwischen sog. Cloud- und Edge-Diensten erleichtert wird,

- Schutzvorkehrungen gegen die unrechtmäßige Datenübermittlung ohne Meldung durch Cloud-Diensteanbieter eingeführt werden und

- Interoperabilitätsstandards für Daten, die von anderen Sektoren weiterverwendet werden sollen, entwickelt werden, um Hindernisse für die gemeinsame Nutzung von Daten über bereichsspezifische gemeinsame europäische Datenräume hinweg im Einklang mit den sektorspezifischen Interoperabilitätsanforderungen und Hindernisse für die Nutzung von

[1] Vorschlag für eine Verordnung des Europäischen Parlamentes und des Rates über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz) vom 23.02.2022, COM (2022) 68 final, 2022/0047 (COD), S. 3, online abrufbar unter https://ec.europa.eu/commission/presscorner/detail/de/ip_22_1113, Datum des letzten Abrufs: 29.03.2022.

anderen Daten zu beseitigen, die nicht in den Geltungsbereich eines spezifischen gemeinsamen europäischen Datenraums fallen[2].

III. Stellungnahme der Beteiligten

Im Folgenden werden die Positionen der beteiligten **Beiratsmitglieder** und die Anmerkungen der **Clearingstelle** zu einzelnen Aspekten des Datengesetz dargestellt, auf bürokratische Lasten hingewiesen und – wenn möglich – mittelstandsfreundlichere, bürokratieärmere Regelungsalternativen aufgezeigt beziehungsweise Hinweise erteilt.

1. Allgemeine Positionen der Beteiligten

Die **AG KSpV** stellt dar, dass der Data Act insbesondere zivilrechtliche Rahmenbedingungen für Zugangsrechte zu Nutzerdaten schaffen soll und dass anerkannt werde, dass der Data Act auf eine Öffnung der Datenverarbeitung insbesondere im Verhältnis von Unternehmen zueinander und zu Nutzern abzielen soll. Dabei soll er die Grundlagen für eine übergreifende Data Economy legen, die Anbieterwechsel erleichtern und Auskunftsrechte stärken soll. Hierzu würden auch insbesondere das Recht der Nutzer auf den Zugang und die Nutzung der übermittelten Daten, aber auch das Verbot unfairer Vertragsklauseln zählen.

Seitens der **AG KSpV** wird darauf hingewiesen, dass aufgrund der beschränkten Betroffenheit der Kommunen lediglich zu den Aspekten aus Kapitel 1 (Begriffsbestimmungen) und Kapitel 5 (Bereitstellung von Daten für öffentliche Stellen und Organe, Einrichtungen und sonstige Stellen der Union wegen außergewöhnlicher Notwendigkeit) Anmerkungen dieser erfolgen.

Die **IHKN** teilt mit, dass der Data Act grundsätzlich begrüßt werde, sofern das Ziel, signifikant hohe Potentiale aus der Verwertung von bisher ungenutzten Industriedaten (dem Vernehmen nach 80 %) wertschöpfend für die Wirtschaft zu generieren, durch diese Verordnung gelinge. Zudem findet auch das grundsätzliche Ansinnen, den Wert dieser Daten auch für KMU besser nutzbar zu machen, Zuspruch bei der **IHKN**. Die **IHKN** weist jedoch darauf hin, dass der Entwurf in seiner weitgehend theorielastigen Tendenz bei Weitem noch nicht konkret und praxisorientiert genug sei, um allen Beteiligten die Mechanismen und die Systematik in der Praxis klar und umsetzbar vor Augen zu führen. Falls der Entwurf in erster Linie den KMU zugutekommen soll, dürfte gerade dieser Gruppe durch eine zu hohe Komplexität ein Bärendienst erwiesen sein, meint die **IHKN**. Die **IHKN** führt zudem an, dass hierdurch stattdessen eher sog. „Gatekeeper“ in der Regel weitaus größere Kapazitäten hätten, um die Verordnung in die Praxis umzusetzen.

Weiter betont die **IHKN**, dass trotz der guten Absicht, KMU an der Wertschöpfungskette besser teilhaben zu lassen, ein großer Teil des Entwurfs so unscharf und theoretisch sei, dass in der

[2] Vorschlag für ein Datengesetz, COM (2022) 68 final, 2022/0047 (COD), a.a.O., S. 3f..

Praxis ein ganz erheblicher Beratungsbedarf entstünde. Dieser Umstand würde die beabsichtigten Vorteile um ein Vielfaches übersteigen.

Aus Sicht des Handwerks (**LHN** und **UHN**) sei der Data Act grundsätzlich zu begrüßen, da ein fairer Zugang zu Daten für Handwerksbetriebe von zentraler Bedeutung sei. Wichtig sei insbesondere der Zugang zu technischen oder kundenbezogenen Daten, die Wartungs- oder Reparaturleistungen ermöglichen. **LHN** und **UHN** begrüßen, dass mit dem Data Act der Grundsatz verankert werde, dass Daten, die für die Nutzung von Produkten und damit verbundenen Dienstleistungen entstehen, generell zugänglich gemacht werden müssen, um einen fairen Wettbewerb sicherzustellen. Aus Handwerkssicht wird außerdem positiv bewertet, dass der Nutzer entscheiden kann, seine Daten auch mit unabhängigen Dritten zu teilen, damit diese sein Produkt reparieren und warten oder weitere Dienstleistungen erbringen können. Darüber hinaus begrüßen **LHN** und **UHN**, dass der Data Act klare Regeln für den B2B-Datenzugang enthalte, durch welchen es Handwerksbetrieben möglich sei, beispielsweise Verträge mit den Herstellern abzuschließen, um den Zugang zu Daten zu erhalten. Da die Verhandlungsmacht der Hersteller wesentlich größer sei als die der KMU, werde von **LHN** und **UHN** außerdem die Fairness-Prüfung im B2B-Bereich begrüßt, die vorsieht, dass missbräuchliche Vertragsklauseln gegenüber KMU im Zusammenhang mit dem Zugang zu Daten und deren Nutzung unwirksam sind.

UVN teilt zum Data Act mit, dass sich dieser vorteilhaft auf den Austausch von industriellen Daten über Unternehmens- und Sektorgrenzen auswirken und so die Entwicklung von datengetriebenen Geschäftsmodellen erleichtern könne, sofern dieser konsequent auf Datenzugang und -nutzung ausgerichtet werde. In seiner aktuellen Ausgestaltung blieben jedoch auch aus Sicht von **UVN** noch zu viele Fragen ungeklärt, was zu mehr Unsicherheit als Sicherheit führen dürfte.

2. Konkrete Positionen der Beteiligten

Im Folgenden sollen die einzelnen, vorgesehenen Regelungen näher betrachtet werden:

a. Kapitel I: Allgemeine Bestimmungen

Mit Kapitel I werden Gegenstand und Anwendungsbereich der Verordnung sowie die Begriffsbestimmungen für den Rechtsakt festgelegt.

So enthält das Datengesetz gemäß Art. 1 Abs. 1 Vorschriften über die Bereitstellung von ***Daten, die bei der Nutzung eines Produktes oder verbundenen Dienstes erzeugt werden, für den Nutzer dieses Produktes oder Dienstes, über die Bereitstellung von Daten durch Dateninhaber für öffentliche Stellen oder Organe, Einrichtungen und sonstige Stellen der Union, soweit diese Daten wegen außergewöhnlicher Notwendigkeit zur Wahrnehmung einer Aufgabe von öffentlichem Interesse benötigt werden*.**

Das Datengesetz gilt für ***Hersteller*** von Produkten und **Erbringer** verbundener Dienste, die in der Union in Verkehr gebracht werden, für die ***Nutzer*** solcher Produkte oder Dienste, für ***Dateninhaber***, die Datenempfängern in der Union Daten bereitstellen, ***Datenempfänger*** in der Union, denen Daten bereitgestellt werden, ***öffentliche Stellen*** und ***Anbieter von Datenverarbeitungsdiensten***, die Kunden in der Union solche Dienste anbieten (Art. 1 Abs. 2 Datengesetz).

In Art. 2 Datengesetz werden die ***wesentlichen Begriffe definiert***, was vorteilhaft ist, denn so ist es möglich, die Rechte und Pflichten nachzuvollziehen. Sofern es hinsichtlich der Begrifflichkeiten Unklarheiten gibt, wird hierauf in den einzelnen, konkreten Regelungen noch einmal genauer eingegangen.

Auch die **IHKN** weist darauf hin, dass eine vorangestellte Definition von Begriffen hilfreich sei und der Orientierung dienen könne. Im Hinblick auf Art. 2 Nr. 1 sei allerdings unklar, warum eine nähere Spezifizierung der Datengüte unterbliebe. Nach Ansicht der **IHKN** ziele der Entwurf in erster Linie auf nicht personenbezogene Daten (vgl. Art. 5 Abs. 6) ab, insbesondere auf Industriedaten. Da personenbezogene und nicht personenbezogene Daten im Hinblick auf deren Verarbeitung sehr unterschiedlichen Reglementarien unterliegen würden, befürchtet die **IHKN**, dass es in der Folge zu starken Verwerfungen kommen könnte, wenn hier nicht klar unterschieden werde. Die **IHKN** führt hierzu aus, dass das volle Reglement des Datenschutzes greife, sobald Daten personenbezogen sind, sei es unmittelbar oder indirekt durch eine Pseudonymisierung. Beispielsweise seien technische Daten aus einem PKW, die der Nutzer unentwegt erzeugt, allesamt personenbezogen, wenn diese ihm als Person direkt oder mittelbar zugeordnet werden können (z.B. Fahrverhalten, Verschleiß, Verbrauch, Fahrzeiten, Wege usw.). Diese Daten seien bei weitem nicht in dem Maße verwertbar, wie es bei nicht personenbezogenen Daten der Fall wäre. Die **IHKN** regt daher an, dass bereits an dieser Stelle zumindest geklärt werden sollte, dass personenbezogene Daten nicht gemeint seien.

Nicht ersichtlich ist zudem aus Sicht der **Clearingstelle**, warum das Datengesetz nur für Daten gelten soll, die durch die Nutzung eines Produktes oder einer damit verbundenen Dienstleistung entstehen, da durch die Nutzung von Online- und mobilen Diensten erzeugte Daten (zum Beispiel Standortdaten aus Apps) von gleichem Wert sind[3].

[3] so auch *Bousonville*, EU-Data Act: Kommission schlägt neue Regeln für den Datenaustausch vor, Beitrag vom 09.03.2022, online abrufbar unter: https://www.pinsentmasons.com/de-de/out-law/nachrichten/eu-data-act-new-rules-for-data-exchanges, Datum des Abrufs: 31.03.2022.

b. Kapitel II: Datenweitergabe von Unternehmen an Verbraucher und zwischen Unternehmen

Die Regelungen in Kapitel II zielen darauf ab, die Rechtssicherheit für Verbraucherinnen und Verbraucher sowie Unternehmen beim Zugang zu Daten zu erhöhen, welche durch Produkte oder verbundene Dienste erzeugt werden, die sie besitzen, mieten oder leasen[4].

aa. Art. 3 Abs. 1 Datengesetz – Pflicht der Zugänglichmachung

Im Zusammenhang mit der Zugangsgewährung, stellt sich die Frage, welche Daten genau erfasst werden müssen, welche Daten benötigt werden, in welchem Format die Daten wann zugänglich zu machen sind und wenn Daten benötigt werden, wie aktuell die Daten sein müssen und in welcher Frequenz diese zu aktualisieren sind[5].

Art. 3 Abs. 1 Datengesetz sieht vor, dass Produkte so konzipiert und hergestellt und verbundene Dienste so erbracht werden müssen, dass ***die bei ihrer Nutzung erzeugten Daten standardmäßig für den Nutzer einfach, sicher*** und – soweit relevant und angemessen – ***direkt zugänglich*** sind.

Die Begriffe „Produkt“ und „verbundener Dienst“ sind in Art. 2 Nr. 2 sowie Nr. 3 Datengesetz aus Sicht der **Clearingstelle** nachvollziehbar definiert.

Die **IHKN** regt in diesem Zusammenhang jedoch an, dass an dieser Stelle auch das Stichwort „Access by design“ beziehungsweise „Zugang durch Technikgestaltung“ Erwähnung finden sollte.

„Nutzer“ ist gemäß Art. 2 Nr. 5 Datengesetz eine ***natürliche oder juristische Person, die ein Produkt besitzt, mietet oder least oder eine Dienstleistung in Anspruch nimmt***. Da der Besitz einer Sache (tatsächliche Sachherrschaft) bei einer mietvertraglichen Überlassung oder einer Überlassung im Wege des Leasings grundsätzlich auf den Mieter beziehungsweise Leasingnehmer übertragen wird, kann zunächst davon ausgegangen werden, dass statt „besitzt“, *„kauft“* (Eigentumserwerb) gemeint sein soll. Hierfür spricht auch, dass im Erwägungsgrund 16 von Kauf-, Miet- und Leasingverträgen die Rede ist und in Erwägungsgrund 18 ebenfalls aufgeführt ist, dass der Nutzer eine natürliche oder juristische Person ist, die das Produkt *gekauft hat*. Hierin heißt es weiter, dass die Person des Nutzers, je nach dem Rechtstitel, unter dem er es nutzt, die Risiken trägt und die Vorteile des vernetzten Produkts genießt und daher auch Zugang zu den Daten haben und mithin berechtigt sein sollte, aus den von diesem Produkt und allen verbundenen Diensten erzeugten Daten Nutzen zu ziehen.

[4] Vorschlag für ein Datengesetz, COM (2022) 68 final, 2022/0047 (COD), a.a.O., S. 18.
[5] siehe *Podzun*, Handwerk in der digitalen Ökonomie, Rechtlicher Rahmen für den Zugang zu Daten, Software und Plattformen, 1. Auflage, 2021, S. 162 f..

Diesbezüglich regt die **Clearingstelle** eine Korrektur der Regelung beziehungsweise der deutschsprachigen Übersetzung an.

Probleme im Hinblick auf den Nutzerbegriff könnten sich zudem daraus ergeben, dass bei mehreren Nutzern eines Produktes nicht immer eindeutig klar ist, wem welche Daten bereitgestellt werden müssen (Bsp. Ärzt:innen und Patient:innen, die ein Produkt nutzen)[6].

Fraglich ist außerdem, wann die bei der Nutzung erzeugten Daten standardmäßig für den Nutzer ***einfach***, ***sicher*** und – soweit relevant und angemessen – ***direkt zugänglich*** sind. Hinweise zur Antwort auf diese Frage lassen sich den Erwägungsgründen 20 ff. entnehmen. Hier werden zum Beispiel Anforderungen an Produkte, auf welche mehrere Nutzer Zugriff haben, festgelegt. Allerdings sind die Bestimmungen sehr vage gehalten. So

- *„sollten **angemessene Anstrengungen** bei der Konzeption des Produkts oder verbundenen Dienstes oder der entsprechenden Schnittstelle unternommen werden, damit alle Personen Zugang zu den erzeugten Daten haben“,*
- Hersteller „sollten ***den erforderlichen Mechanismus*** *einrichten, der getrennte Nutzerkonten (…) ermöglicht*“,
- *„der Zugang sollte dem Nutzer mit Hilfe **einfacher Verfahren** gewährt werden, die eine **automatische Ausführung** ermöglichen und keine Prüfung durch den Hersteller oder Dateninhaber erfordern“,*
- Daten sollen nur *„bereitgestellt werden, wenn der Nutzer dies **tatsächlich wünscht**“,*
- sofern eine automatische Ausführung des Datenzugangsverlangens nicht möglich ist, *„sollte der Hersteller den Nutzer darüber informieren**, wie auf die Daten zugegriffen werden kann**.“.*

Es ist nicht davon auszugehen, dass mit der Regelung in Art. 3 Abs. 1 Datengesetz sowie unter Zugrundelegung der Erwägungsgründe gewährleistet werden kann, dass die Hersteller als Dateninhaber rechtssicher ihrer Pflicht zur Zugänglichmachung von Daten nachkommen können.

Aus Sicht von **LHN** ist die Schaffung technischer Voraussetzungen zur Datennutzung essentiell. Daher müssen Schnittstellen vorhanden sein, damit Nutzer der jeweiligen Geräte, allen Unternehmen die Erlaubnis zum Auslesen und Analysieren der Daten erteilen können und damit die Dienstleister mit den Kunden in Kontakt treten können. Dies ist bei einer Konkretisierung der Pflichten mithin zu berücksichtigen.

Unbestimmte Rechtsbegriffe führen bei Unternehmen zu mehr zeitlichem und finanziellem Aufwand, da diese eigenständig oder auch unter Rückgriff auf fremde Expertise hinterfragt und ausgelegt werden müssen. Sofern sich unbestimmte Rechtsbegriffe nicht vermeiden lassen, so sollten zumindest schnell auffindbare, rechtsverbindliche Erläuterungen zur Hand gegeben werden, die unterstützend von den Regelungsadressaten herangezogen werden können. Falls

[6] *Johner*, EU Data Act: Hosen runter!, Artikel vom 22.03.2022, online abrufbar unter https://www.johner-institut.de/blog/regulatory-affairs/eu-data-act/, Datum des letzten Abrufs: 31.03.2022.

im weiteren Verlauf dann ersichtlich wird, dass die Rechtsbegriffe fehlerhaft ausgelegt werden, sollten die hilfestellenden Handreichungen unverzüglich angepasst werden.

Die **IHKN** bestätigt diese Annahme und gibt ebenfalls zu bedenken, dass aufgrund der zahlreichen unbestimmten Rechtsbegriffe und der noch zahlreicheren unbestimmten Anforderungen gerade für KMU nicht nur erhebliche Mehrbelastungen durch externen Beratungsbedarf entstehen würden, sondern diese auch dazu führen würden, dass eine ausreichende Güte der jeweiligen Beratungsleistungen durch die hohe Rechtsunsicherheit nicht gewährleistet werden könne. Es sei daher naheliegend, dass KMU trotz entsprechender Beratungsinvestitionen falsche Entscheidungen treffen werden. Etwaige Beratungsfehlleistungen müssten nach Ansicht von **IHKN** zudem zumindest durch Versicherungen abdeckbar sein. Außerdem weist die **IHKN** darauf hin, dass ein ähnliches Problem auch in der DSGVO, konkret aufgrund Art. 25 DSGVO „Privacy by Design“, bestehe und bisher nicht von allen Unternehmen umgesetzt werde.

Aus den praktischen Erfahrungen mit der Datenschutz-Grundverordnung (DSGVO) soll sich zudem ableiten lassen, dass mit erheblich gestiegenen Compliance-Anforderungen ein hohes Maß an Rechtsunsicherheit bei den Unternehmen im Zusammenhang mit der Auslegung neuer Rechtsbegriffe sowie der Abgrenzung unterschiedlicher Rechtsakte untereinander (im vorliegenden Fall insbesondere zwischen der DSGVO und dem Datengesetz) besteht[7]. Die **IHKN** weist diesbezüglich darauf hin, dass datenschutzrechtliche Fragestellungen über das Gesetz selbst zu klären seien, da diese ansonsten zu Rechtsunsicherheit und in der Folge dazu führen würden, dass Unternehmen davon Abstand nehmen würden, Daten untereinander auszutauschen. Hierdurch würden die wirtschaftlichen Potentiale des Data Acts laut **IHKN** zumindest stark gehemmt werden.

Aufgrund der Pflicht zur Zugänglichmachung wird außerdem eine Vielzahl von Unternehmen ihre Produkte in jedem Fall insofern ändern müssen, als dass die Produkte Schnittstellen anbieten, die die Vorgaben an die Interoperabilität erfüllen und die Daten auch unter den entsprechenden Anforderungen des Datengesetzes bereitstellen können (siehe hierzu auch die Ausführungen von **LHN** weiter oben sowie unter Abschnitt III. 2. h. dieser Stellungnahme)[8].

Eine unreflektierte Zugangsermöglichung zu Daten könnte möglicherweise insofern nicht zielführend sein, als dass für das Handwerk zum Beispiel vielmehr die Ermöglichung der Leistungserbringung, der unmittelbare Zugang zur Leistungserbringung sowie der Zugang zu Kooperationen relevant ist und eine schnelle und praktikable Klärung der Bedingungen für eine Eröffnung des Zugangs zu Daten entscheidend für die Möglichkeit einer wirksamen Geltendmachung von Ansprüchen auf Zugang ist[9].

[7] *Schumacher/von Schönfeldt/Bartels*, „Die Datenstrategie der EU: Das Datenrecht als neues Rechtsgebiet?“, Gastbeitrag für Legal Tribune Online (LTO) vom 21.03.2022, online abrufbar unter https://www.lto.de/recht/hintergruende/h/uebersicht-gesetze-regeln-datenrecht-datenschutz-datenstrategie-eu-data-act-free-flow-of-data-act/, Datum des letzten Abrufs: 01.04.2022.
[8] *Johner*, a.a.O..
[9] siehe *Podzun*, a.a.O., S. 8 f..

Ferner ist zu berücksichtigen, dass viele Unternehmen mit (Roh-)Daten nichts anfangen können[10]. Da eine Vielzahl von Unternehmen und Betrieben, seien es Bäckereibetriebe oder Orthopädietechniker, keine IT-Unternehmen oder Data-Scientisten sind, ist die Bereitstellung dieser nicht immer zielführend[11]. Es sollte der Regelung daher entnommen werden können, was mit „Zugang" genau gemeint und unter welchen Voraussetzungen und zu welchen Bereichen dieser Zugang zu Daten zu erteilen ist[12]. In der Regel ist nämlich nicht der Zugang zu Rohdaten relevant, sondern den Unternehmen muss es ermöglicht werden, Zugang zu Informationen zu erhalten, die für die konkrete Bearbeitung eines Auftrags (zum Beispiel Reparatur eines Gegenstands, Wartung einer vernetzten Heizung, Ausbau eines Smart Homes) notwendig sind[13]. Es sollten – sofern möglich – auch die Formen und Bedingungen für die Bereitstellung der Daten geregelt[14] und technische Lösungen mitgedacht werden, um Handlungsmöglichkeiten lösungsorientiert zu erweitern und Innovationen zu incentivieren[15]. Zudem dürfen technische Lösungen nicht zu komplex oder mit hohen Anfangsinvestitionen verbunden sein[16].

Das „Wie" des Zugangs ist nämlich insbesondere auch für Gewährleistungs- und Haftungsfragen relevant. Da für die wertschöpfende Verwendung von Daten auch deren richtige Darstellung und Lesbarkeit entscheidend ist, sollte der Mängelbegriff für die Zugänglichmachung und die Eigenschaften von Daten ausreichend definiert und so entsprechende Standards verbindlich festgelegt werden. Hierzu sollten die Unternehmensvertreter der betroffenen Branchen konkret befragt und in die Erarbeitung eingebunden werden[17], gegebenenfalls könnte ein Zugang über Kooperationen und Verbände ermöglicht werden[18].

bb. Art. 3 Abs. 2 Datengesetz – vorvertragliche Informations- und Transparenzpflichten

Gemäß Art. 3 Abs. 2 Datengesetz hat der Hersteller **vor Abschluss eines Kauf-, Miet- oder Leasingvertrags** dem Nutzer gegenüber **verschiedene Informations- und Transparenzpflichten** zu erfüllen.

Diese vorvertraglichen Aufklärungspflichten im Hinblick auf Einzelheiten der Datennutzung und bestehende Nutzungsrechte ähneln denen der DSGVO[19].

[10] siehe *Podzun*, a.a.O., S. 106.
[11] *Podszun*, a.a.O., S. 106.
[12] siehe *Podzun*, a.a.O., S. 106.
[13] Ebenda.
[14] Siehe hierzu auch *Podzun*, a.a.O., S. 111.
[15] *Podzun*, a.a.O., S. 126.
[16] *Podzun*, a.a.O., S. 160f..
[17] *Podzun*, a.a.O., S. 144f.
[18] *Podzun*, a.a.O., S. 160f..
[19] *Heynicke/Schönhagen*, KPMG-Law, Mandanten-Information, IT- und Datenschutzrecht, Februar 2022, online abrufbar unter https://kpmg-law.de/mandanten-information/key-facts-zum-neuen-entwurf-des-data-act/, Datum des letzten Abrufs: 31.03.2022.

Die Pflichten führen unter anderem dazu, dass die betroffenen Unternehmen ihre Produktgestaltungen, Produktunterlagen und etwaig weitere dazugehörige Vertragsgrundlagen sowie Allgemeine Geschäftsbedingungen überarbeiten (lassen) müssen.

Insbesondere muss das Unternehmen zum Beispiel in dem Fall, in dem es selbst zwar Verkäufer, Vermieter oder Leasinggeber jedoch nicht Dateninhaber[20] ist, die Identität des Dateninhabers, zum Beispiel seinen Handelsnamen und die Anschrift der Niederlassung, bereitstellen (Art. 3 Abs. 2 lit. e Datengesetz). Dies stellt einen erheblichen Aufwand dar, da es keine eigenen, sondern fremde Informationen sind, deren Aktualität immer auch nachgehalten werden muss. Da fehlende beziehungsweise fehlerhafte Produktinformationen immer auch abmahnfähige Wettbewerbsverstöße darstellen können, die entsprechende Kosten und weiterführende Risiken (Abgabe von strafbewehrten Unterlassungserklärungen, bei Folgeverstößen Vertragsstrafeforderungen) bergen, bringen Pflichten zur Bereitstellung entsprechender Informationen immer auch eine (bürokratische) Belastung auf Seiten der betroffenen Unternehmen mit sich.

Die Bereitstellung der Informationen hat in einem ***klaren und verständlichen Format*** zu erfolgen. Welche Anforderungen genau an das Format sowie an dessen „Klarheit“ und Verständlichkeit zu stellen sind, bleibt unklar. Grundsätzlich können hier hinsichtlich der Ausgestaltung sicherlich aufgrund anderer Vorschriften begründete Transparenz- und Informationspflichten herangezogen werden, auch dies führt in der Regel jedoch dazu, dass die betroffenen Unternehmen (externe) rechtliche Expertise heranziehen müssen und Haftungsproblematiken entstehen können.

Die **IHKN** bestätigt diese Auffassung und ergänzt, dass eine eigene Expertise in der Regel nur die sog. „Gatekeeper“ haben werden. Auch durch diese unbestimmten Rechtsbegriffe würden die KMU einen erheblichen Beratungsbedarf haben, der die vermeintlichen Vorteile der Verordnung – zumindest in den ersten Jahren – weit übertreffen würde.

Auch hier sollte daher eine Konkretisierung erfolgen. Alternativ könnte ein Leitfaden mit Hilfestellungen in Bezug auf die notwendigen Informationen für die betroffenen Unternehmen nützlich sein. Einen solchen würde auch **LHN** begrüßen.

Darüber hinaus sollen dem Nutzer vor Abschluss eines Kauf-, Miet- oder Leasingvertrags für ein Produkt oder verbundenen Dienst die Informationen über die Kommunikationsmittel bereitgestellt werden, mit denen der Nutzer den Dateninhaber schnell kontaktieren und **effizient** mit diesem kommunizieren kann. Es ist nicht ersichtlich, was in diesem Zusammenhang unter dem Wort „effizient“ verstanden werden kann. Aus Sicht der **Clearingstelle** wäre es zielführend, wenn den Dateninhabern Informationen bereitgestellt

[20] *Anm. d. Verf.:* Dateninhaber ist gemäß Art. 2 Nr. 6 Datengesetz eine juristische oder natürliche Person, die (…) berechtigt und verpflichtet bzw. im Falle nicht personenbezogener Daten und durch die Kontrolle über die technische Konzeption des Produktes und damit verbundener Dienste in der Lage ist, bestimmte Daten bereitzustellen.

werden, welche Kommunikationsmittel in diesem Zusammenhang als „effizient“ angesehen werden.

Zudem ist der Nutzer über sein Recht zur Beschwerde wegen eines Verstoßes gegen Herstellerpflichten nach dem Datengesetz bei der in Art. 31 genannten zuständigen Behörde aufzuklären (Art. 3 Abs. 2 lit. h Datengesetz). Diese Regelung erinnert an die Verordnung über Online-Streitbeilegung in Verbraucherangelegenheiten (ODR-Verordnung), die ab Anfang 2016 für außergerichtliche Beilegung von Streitigkeiten zwischen Verbrauchen und Unternehmern in der EU gilt und deren Ziel es war, eine Online-Streitbeilegungsplattform (OS-Plattform) auf Unionsebene zu schaffen und die Zusammenarbeit mit den nationalen Stellen für die alternative Streitbeilegung (AS-Stellen gemäß ADR-Richtline) regeln sollte[21]. Aufgrund dieser Verordnung müssen in der Union niedergelassene Unternehmen, die Online-Kaufverträge oder Online-Dienstverträge eingehen, auf ihren Websites einen Link zur OS-Plattform bereitstellen, der für Verbraucher leicht zugänglich und anklickbar sein muss, sofern sie sich dazu verpflichtet haben oder gesetzlich verpflichtet sind.

Aufgrund dessen, dass auch das Datengesetz vorsieht, dass der Unternehmer dem Nutzer vor Vertragsschluss die konkrete Behörde zu benennen hat, bei der dieser Beschwerde einlegen kann, um Verstöße gegen das Datengesetz zu melden, ist davon auszugehen, dass der Unternehmer auch hier seine Allgemeinen Geschäftsbedingungen entsprechend anpassen muss, was voraussichtlich ebenfalls dazu führen wird, dass ihm neben zeitlichen Aufwänden auch Kosten entstehen werden, sofern er für die Überarbeitung Rechtsberatung in Anspruch nimmt, um in Erfahrung zu bringen, wie (Wortlaut) und an welcher Stelle (Ort) die Information zu erbringen ist. Diese Rechtsunsicherheiten birgen ebenfalls wettbewerbsrechtliche Risiken für Unternehmerinnen und Unternehmer.

Möglicherweise könnte die Regelung auch zu Abgrenzungsproblematiken bei den Adressaten führen, da für sie nicht ersichtlich ist, welche Stelle für eine Beschwerde beziehungsweise einen Streitfall zuständig ist, was dann auch zumindest mittelbar eine bürokratische Last bei den betroffenen Unternehmen (Dateninhaber, Nutzer und Datenempfänger) darstellen würde.

Auch die **IHKN** sieht es so, dass es für Nutzer kaum überschaubar sein dürfte, welche Plattform für welche Angelegenheit zu nutzen ist. Deshalb bestehe die Gefahr, dass Beschwerden an die falschen Ansprechpartner gesendet werden und dann ins Leere laufen. Außerdem werde mit der Schaffung einer weiteren Plattform beziehungsweise Behörde auch eine weitere Belastung für Unternehmen geschaffen, die hinsichtlich der Belehrung und Aktualität wieder Rechtsunsicherheit schaffen würde.

[21] Verordnung (EU) Nr. 524/2013 des Europäischen Parlaments und des Rates vom 21.05.2013 über die Online-Beilegung verbraucherrechtlicher Streitigkeiten und zu Änderung der Verordnung (EG) Nr. 2006/2004 und der Richtlinie 2009/22/EG (Verrordnung über Online-Streitbeilegung in Verbraucherangelegenheiten), online abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32013R0524&from=DE, Datum des letzten Abrufs: 29.03.2022.

cc. Art. 4 Abs. 1 Datengesetz – Recht der Nutzer auf Zugang zu den Daten

Nach Art. 4 Abs. 1 Datengesetz hat der Dateninhaber dem Nutzer – soweit dieser nicht direkt vom Produkt auf die Daten zugreifen kann – die bei der Nutzung eines Produkts oder verbundenen Dienstes erzeugten Daten ***auf einfaches Verlangen unverzüglich, kostenlos und gegebenenfalls kontinuierlich und in Echtzeit*** zur Verfügung zu stellen. Die Zurverfügungstellung hat ***auf elektronischem Wege*** zu erfolgen, soweit technisch machbar.

Erwägungsgrund 28 ist zu entnehmen, dass es dem Nutzer freistehen soll, die Daten für jeden rechtmäßigen Zweck zu verwenden und dass der Dateninhaber sicherstellen soll, dass die den Dritten bereitgestellten Daten ***so genau, vollständig, zuverlässig, relevant und aktuell sind, wie die bei der Nutzung des Produkts oder verbundenen Dienstes erzeugten Daten, auf die der Dateninhaber selbst zugreifen kann oder darf***.

Die **IHKN** meint hierzu, dass diese Regelung für Unternehmen kaum nachvollziehbar sein und daher auch zu Rechtsunsicherheiten führen dürfte.

dd. Art. 4 Abs. 2 Datengesetz – Informationsverlangen des Dateninhabers

Der Dateninhaber darf vom Nutzer ***keine Informationen verlangen, die über das hinausgehen, was erforderlich ist, um dessen Eigenschaft als Nutzer zu überprüfen*** und ***keine Informationen über den Zugang des Nutzers zu den verlangten Daten aufbewahren, die über das hinausgehen, was für die ordnungsgemäße Ausführung des Zugangsverlangens des Nutzers und für die Sicherheit und Pflege der Dateninfrastruktur erforderlich ist***.

Hierzu ist dem Erwägungsgrund 27 zu entnehmen, dass es dem Dateninhaber zur Prüfung der Berechtigung des Nutzers auf Zugang zu den Daten möglich sein soll, eine ***geeignete Nutzeridentifizierung*** zu verlangen. Welche Anforderungen an die Nutzeridentifizierung genau zu stellen sind, damit diese „geeignet“ ist, bleibt unklar. Auch hier wird von der **Clearingstelle** eine Konkretisierung angeregt.

Bei der Bedienung eines Auftragsverarbeiters hat der Dateninhaber zudem sicherzustellen, dass das ***Zugangsverlangen vom Auftragsverarbeiter empfangen und bearbeitet*** wird (Erwägungsgrund 27). Da dies den Umfang der Leistungen, die der Auftragsverarbeiter für den Dateninhaber erbringen soll, erweitern wird, werden durch diese Verpflichtung auf Seiten des Dateninhabers regelmäßig höhere Kosten entstehen.

ee. Art. 4 Abs. 3 Datengesetz – Geschäftsgeheimnisse

Art. 4 Abs. 3 Datengesetz bestimmt, dass ***Geschäftsgeheimnisse nur offengelegt werden, wenn alle besonderen Maßnahmen getroffen worden sind, die erforderlich sind, um die Vertraulichkeit der Geschäftsgeheimnisse***, insbesondere gegenüber Dritten, ***zu wahren***. Dabei soll es möglich sein, dass Dateninhaber und Nutzer Maßnahmen vereinbaren, um die Vertraulichkeit der gemeinsam genutzten Daten, insbesondere gegenüber Dritten, zu wahren.

Aus Sicht der **Clearingstelle** erscheint fraglich, ob dies überhaupt in der Praxis gewährleistet werden kann und wenn ja, wie genau. Diesbezüglich stellt die **IHKN** dar, dass dies eine der großen, offenen Fragen des Entwurfes sei. Im Zweifel handele es sich bei jedem technischen Datum um ein Betriebsgeheimnis. Obendrein sei ein solches in der Regel auch personenbezogen. Es müsse daher zunächst eine klare Abgrenzung definiert werden, wann ein Datum rein technischer Natur, aber noch kein Betriebsgeheimnis ist. Erst dann könne man sich der Frage widmen, welche Maßnahmen erforderlich sind. Beides ist nach Ansicht der **IHKN** völlig unklar. Außerdem stellt die **IHKN** in diesem Zusammenhang die Frage, wer die Verantwortung hierfür trägt. Diese Anforderungen dürften jedes KMU überfordern. Möglicherweise könnten Musterklauseln einen Ansatz für eine praktikable Lösung darstellen, aber es scheitere der **IHKN** zufolge an einer klaren, praktisch handhabbaren Definition des schützenswerten Geschäftsgeheimnisses.

Fraglich sei nach Auffassung der **IHKN** auch, in welcher Form eine Vereinbarung zwischen Dateninhaber und Nutzer erfolgen soll. Die Unterzeichnung einer schriftlichen Vereinbarung sei zu umständlich und zeitintensiv. Das einfache Anklicken eines Links sei jedoch nicht rechtssicher. Zu prüfen wäre, ob eine sog. „Double Opt-in“-Lösung Rechtssicherheit schaffen könnte, so **IHKN**.

UVN betont diesbezüglich, dass bei der Weitergabe von Daten zu jeder Zeit sichergestellt sein müsse, dass Geschäftsgeheimnisse nicht weitergegeben und von Dritten abgegriffen werden. Wie dies gewährleistet werden kann, zeigten bereits die Unternehmen der Elektro- und Digitalindustrie. Diese würden heute bereits sektorspezifische Lösungsbausteine anbieten, die das sichere Teilen von Maschinendaten über Teilmodelle der Verwaltungsschale ermöglichen würden. Einen anderen Weg stellten Datentreuhändermodelle im Bereich der Gesundheitswissenschaft dar.

Unklar ist in diesem Zusammenhang ferner, welche Anforderungen an einen Nachweis, die der Hersteller zu erbringen hat, um begründen zu können, dass seine Geschäftsgeheimnisse gefährdet sind, zu stellen sind[22].

[22] *Johner*, a.a.O.

ff. Art. 4 Abs. 4 Datengesetz – Wettbewerb

Die Daten, die vom Nutzer herausverlangt wurden, dürfen von diesem ***nicht zur Entwicklung eines Produktes genutzt werden, das mit dem Produkt, von dem die Daten stammen, im Wettbewerb steht***.

Wie dies tatsächlich sichergestellt werden soll, bleibt unklar. Insbesondere ist nicht ersichtlich, ob und wie genau überhaupt vom Dateninhaber festgestellt werden kann, ob ein Nutzer die Daten für die Entwicklung eines Konkurrenzproduktes benutzt hat und wie im Streitfall ein kausaler Schaden bewiesen werden könnte.

Hierzu führt die **IHKN** aus, dass diese Frage direkt an die des Betriebsgeheimnisses anknüpfe. Um sich verordnungskonform zu verhalten, sei eine von drei nebulösen, kumulativen Tatbestandsmerkmalen zu beachten:

1. Betriebsgeheimnis ja/nein?
2. Maßnahmen zu deren Schutz erforderlich und ausreichend?
3. Keine Konkurrenztätigkeit mit diesen Daten möglich und tatsächlich geschehen?

Keines davon werde allerdings im Entwurf in praktikabler Weise gelöst. Zudem dürfte im Prozess der Beweis der Konkurrenzverwertung nur schwer zu führen sein, bestätigt **IHKN**.

gg. Art. 4 Abs. 5 Datengesetz – Personenbezogene Daten

Sofern der ***Nutzer keine von der Datenverarbeitung betroffene Person*** ist, darf der Dateninhaber personenbezogene Daten, die bei der Nutzung eines Produktes oder verbundenen Dienstes erzeugt werden, dem Nutzer nur dann zur Verfügung stellen, wenn eine für die Datenverarbeitung wirksame Rechtsgrundlage, wie etwa die ***Einwilligung*** der betroffenen Person oder ein ***berechtigtes Interesse*** gegeben ist. Dieser Nutzer sollte dann, da er als Datenverantwortlicher im Sinne der Verordnung (EU) 2016/679 gilt, sicherstellen, dass die betroffene Person angemessen über die festgelegten, eindeutigen und rechtmäßigen Zwecke dieser Daten und darüber informiert wird, wie sie ihre Rechte wirksam ausüben kann (siehe hierzu Erwägungsgrund 30).

Die Erfüllung dieser Voraussetzungen durch den Nutzer ist nach Ansicht von **IHKN** völlig utopisch. Um datenschutzrechtliche Verwerfungen von vorneherein auszuschließen, sollten personenbezogene Daten von dem Entwurf völlig ausgeschlossen werden, so die **IHKN**. Die praktische Handhabung des Entwurfs wäre auch schon ohne personenbezogene Daten eine Zumutung für KMU, mit personenbezogenen Daten wäre sie praktisch unmöglich, betont **IHKN**.

Aus Sicht der **IHKN** käme, sofern ein Personenbezug besteht, als alternative Regelungsmöglichkeit nur eine technisch voreingestellte Anonymisierung (nicht nur Pseudonymisierung, siehe hierzu auch Abschnitt III. 2. e. dieser Stellungnahme) in Betracht.

hh. Art. 4 Abs. 6 Datengesetz – Nicht personenbezogene Daten

Art. 4 Abs. 6 Datengesetz sieht vor, dass der Dateninhaber ***nicht personenbezogene Daten***, die bei der Nutzung eines Produktes oder eines Dienstes erzeugt werden, nur auf der Grundlage einer ***vertraglichen Vereinbarung mit dem Nutzer*** nutzen darf.

Nicht personenbezogene Daten (Maschinendaten, die Informationen über die Leistung eines Gerätes, die Zahl bearbeiteter Vorgänge oder den Energieverbrauch wiedergeben; Wetterdaten; Straßendaten) können für handwerkliche und industrielle Anwendungen besonders wichtig sein[23].

Bezüglich der Regelung in Art. 4 Abs. 6 Datengesetz kann dem Erwägungsgrund 24 entnommen werden, dass die ***vertragliche Vereinbarung Teil des Kauf-, Miet- oder Leasingvertrages*** sein kann und dass jede Vertragsbedingung in der Vereinbarung, nach der der Dateninhaber die vom Nutzer eines Produktes oder verbundenen Dienstes erzeugten Daten nutzen darf, für den Nutzer transparent sein sollte. Dies soll auch in Bezug auf den Zweck, für den der Dateninhaber die Daten zu verwenden beabsichtigt, gelten.

Die **IHKN** bestätigt den Eindruck der **Clearingstelle**, dass diese Regelung nicht eindeutig genug ist und stellt außerdem dar, dass die Formulierung den Umkehrschluss zuließe, dass personenbezogene Daten keiner vertraglichen Regelung bedürfen. Die Regelung sei insofern auch nicht praktikabel, da nicht ersichtlich sei, wie bzw. woran die Parteien erkennen sollten, dass die Daten nicht personenbezogen sind. Dies ginge nur durch eine technisch voreingestellte Anonymisierung der Daten, so **IHKN**.

Vertragliche Lösungen können hierbei insofern vorteilhaft sein, als dass sie einzelfallabhängig ausgestaltet werden und die Vertragspartner so einen Interessensaugleich erzielen können. Nachteilhaft sind jedoch die hohen Transaktionskosten, da womöglich für verschiedenste Konstellationen ein eigener Vertrag auszuarbeiten und zu verhandeln ist. Zwar können in diesem Zusammenhang auch Formulare und AGB entwickelt werden, diese können aber dazu führen, dass der Vorteil einer interessennahen Ausgestaltung relativiert wird[24]. Außerdem ist hierbei zu berücksichtigen, dass der Nutzer als Vertragspartner gegebenenfalls nicht die Expertise besitzt, die vertraglichen Regelungen über- und durchschauen zu können und auch hierfür Fachkenntnisse Dritter mit entsprechenden Kostenfolgen in Anspruch nehmen muss.

Darüber hinaus wird in Art. 4 Abs. 6 Datengesetz bestimmt, dass der Dateninhaber solche Daten, die bei der Nutzung des Produktes oder des verbundenen Dienstes erzeugt werden, nicht verwenden darf, um daraus 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

[23] *Podszun*, a.a.O., S. 38.
[24] *Podszun*, a.a.O., S. 69.

könnte. Wie dies tatsächlich gewährleistet werden soll, bleibt nach Auffassung der **Clearingstelle** derzeit noch unklar.

ii. Art. 5 Abs. 1 Datengesetz – Recht auf Weitergabe der Daten an Dritte

Der Dateninhaber hat ***auf Verlangen eines Nutzers oder einer im Namen eines Nutzers handelnden Partei, die bei der Nutzung eines Produktes oder verbundenen Dienstes erzeugten Daten einem Dritten unverzüglich, für den Nutzer kostenlos, in derselben Qualität, die dem Dateninhaber zur Verfügung steht, und gegebenenfalls kontinuierlich und in Echtzeit bereitzustellen***.

Nach Erwägungsgrund 29 kann ein Dritter, dem die Daten bereitgestellt werden, ein Unternehmen, eine Forschungseinrichtung oder eine gemeinnützige Organisation sein.

Zweck dieser Regelung ist es, Start-ups, kleine und mittlere Unternehmen aus traditionellen Branchen und mit weniger entwickelten digitalen Fähigkeiten, die Schwierigkeiten haben, Zugang zu einschlägigen Daten zu erlangen, den Zugriff auf diese zu erleichtern und parallel sicherzustellen, dass die entsprechenden Pflichten so verhältnismäßig wie möglich gefasst werden, um eine Übervorteilung zu vermeiden (Erwägungsgrund 36).

LHN erläutert hierzu, dass dies den Forderungen des Handwerks entspreche, wonach der Nutzer entscheiden sollte, was mit seinen Daten passiere. Nur wenn der Nutzer seine Daten auch mit unabhängigen Dienstleistern teilen könne, sei es diesen oftmals erst möglich, die Produkte zu reparieren und zu warten oder weitere Dienstleistungen anzubieten.

Ein weiterer Aspekt, der bei der Datenweitergabe an Dritte aus Sicht der **Clearingstelle** berücksichtigt werden sollte, ist, dass bestimmte Leistungserbringer, beispielsweise Handwerksbetriebe, bereits jetzt und zukünftig höchst wahrscheinlich noch vermehrt die Schnittstelle zum Kunden verlieren könnten. Wenn sich die zu erbringende Leistung auf ein smartes Gerät oder eine vernetzte Leistung bezieht, würden nur noch solche Anbieter in der Auswahl sein, die Zugang zu dem dahinterstehenden (Daten-)Netzwerk haben[25]. Für die Leistungserbringung wären Unternehmen darauf angewiesen, dass Dritte ihnen Zugang zum Kunden und ggf. Daten/Software zur Verfügung stellen beziehungsweise deren Nutzung ermöglichen[26]. Nach Auffassung der **Clearingstelle** wird das Recht auf die Weitergabe der Daten an Dritte als positiv bewertet, da dies den Wettbewerb der Leistungserbringer, unter denen eine Vielzahl an KMU sein wird, in gewisser Weiser wieder „ermöglicht“ und stärkt.

Um das Wertschöpfungspotential von Industrie- und Maschinendaten vollständig heben zu können, müssten Daten jedoch sowohl zum Nutzer als auch zum Komponentenentwickler fließen können, erläutert **UVN**. Hier dürfe es nach Ansicht von **UVN** keine Ungleichbehandlung mehr geben. Als Beispiel führt **UVN** die Weiterentwicklung heutiger Autobatterien an, die sich

[25] *Podszun*, a.a.O., S. 45f.
[26] *Podszun*, a.a.O., S. 45f.

schneller und kosteneffizienter gestalten ließen, wenn Batteriehersteller besser auf forschungsrelevante Daten aus dem Fahrbetrieb der Fahrzeuge zugreifen könnten.

Die Pflicht zur Bereitstellung der Daten an vom Nutzer autorisierte Dritte wird aber auch zum Ergebnis haben, dass die Anforderungen an die IT-Sicherheit erheblich steigen werden[27]. Dies führt wiederum zu mehr Aufwand und höheren Kosten bei den betroffenen Unternehmen.

jj. Art. 5 Abs. 2 Datengesetz – Gatekeeper

Nach Art. 5 Abs. 2 Datengesetz darf keine Weitergabe von Daten an Unternehmen erfolgen, die als sog. „Gatekeeper" gemäß dem Gesetz über digitale Märkte (Digital Markets Act) gelten. Ein Unternehmen wird als **„Gatekeeper"** eingeordnet, wenn es eine starke wirtschaftliche Position mit erheblichen Auswirkungen auf den Binnenmarkt innehat und in mehreren EU-Ländern aktiv ist, über eine starke Vermittlungsposition verfügt, das heißt eine große Nutzerbasis mit einer großen Anzahl von Unternehmen verbindet oder eine gefestigte und dauerhafte Marktstellung hat (oder bald haben wird), das heißt langfristig stabil ist[28]. Fraglich ist, ob die „Gatekeeper"-Eigenschaften auch immer unmittelbar von den Nutzern, bei denen es sich auch um KMU handeln kann, erkannt wird. Selbst wenn man eine positive Kenntnis der vorgenannten Definition auf Seiten der Nutzer annimmt, erscheint es schwierig, Unternehmen ohne eine – möglicherweise zeitintensive – Prüfung und Abwägung der Kriterien als Gatekeeper einordnen zu können und sicherzustellen, dass angemessen berücksichtigt wird, dass ein solches Unternehmen nicht als zulässiger Dritter i. S. d. Art. 5 des Datengesetzes in Betracht kommt und daher keine Daten an dieses weitergegeben werden dürfen und auch keinem Aufforderungsverlangen eines solchen Unternehmens nachgekommen werden darf beziehungsweise muss.

Auch die **IHKN** sieht dies so und stellt dar, dass diese Anforderung völlig utopisch sei. Sie wäre nur dann praktikabel, wenn die „Gatekeeper" ein scharf eingrenzbares Unterscheidungsmerkmal aufwiesen oder offiziell in einer öffentlichen Tabelle verzeichnet wären, was jedoch aus Sicht der Wirtschaft abzulehnen wäre, so **IHKN**. Die Anregung der **Clearingstelle** dahingehend, dass eine Liste mit „Gatekeepern" öffentlich zugänglich gemacht und aktuell gehalten wird, wird von **LHN** befürwortet. **IHKN** sieht hierdurch jedoch die Gefahr gegeben, dass eine öffentliche Stigmatisierung drohen und das Image der Unternehmen in der öffentlichen Wahrnehmung beschädigt werden könnte.

[27] *Johner*, a.a.O..
[28] Europäische Kommission, Das Gesetz über digitale Märkte: für faire und offene digitale Märkte, Was ist ein Gatekeeper?, online abrufbar unter https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_de, Datum des letzten Abrufs: 25.03.2022.

Ergänzend sei darauf hingewiesen, dass das Verbot zur Datenweitergabe teilweise auch als „Zwangsmaßnahme“ angesehen und diesbezüglich angeführt wird, dass dieses mit dem Grundsatz der Vertragsfreiheit nicht zu vereinbaren sei[29].

kk. Art. 5 Abs. 5 Datengesetz – Technische Möglichkeit, Zustimmung jederzeit zu widerrufen

Art. 5 Abs. 5 Datengesetz sieht vor, dass der Dateninhaber ***nicht personenbezogene Daten***, die bei der Nutzung des Produktes oder verbundenen Dienstes erzeugt werden, ***nicht verwenden darf, um daraus Einblicke in die wirtschaftliche Lage, Vermögenswerte und Produktionsmethoden des Dritten oder in die Nutzung durch den Dritten zu erlangen***, wenn dies die gewerbliche Position des Dritten auf den Märkten, auf denen dieser tätig ist, untergraben könnte, es sei denn, der Dritte hat einer solchen Nutzung zugestimmt und hat die technische Möglichkeit, diese **Zustimmung jederzeit zu widerrufen**. Ob dieses Verbot, die Gefahr, dass Wettbewerber die Daten nutzen, beseitigen kann, ist fraglich. Es ist zudem nicht ersichtlich, wie der Nachweis eines Verstoßes geführt werden kann[30].

ll. Art. 5 Abs. 8 Datengesetz – Offenlegung von Geschäftsgeheimnissen gegenüber Dritten

Art. 5 Abs. 8 Datengesetz bestimmt, dass Geschäftsgeheimnisse Dritten gegenüber nur insoweit offengelegt werden, als dies für den zwischen dem Nutzer und dem Dritten vereinbarten Zweck ***unbedingt erforderlich*** ist und dass der Dritte ***alle zwischen ihm und dem Dateninhaber vereinbarten besonderen Maßnahmen getroffen hat, die erforderlich sind, um die Vertraulichkeit des Geschäftsgeheimnisses zu wahren.*** In diesem Fall sollen die Eigenschaft der Daten als Geschäftsgeheimnisse und die Maßnahmen zur Wahrung der Vertraulichkeit zwischen Dateninhaber und dem Dritten festgelegt werden.

Diesbezüglich wird zunächst auf die obigen Erwägungen verwiesen.

In der Regel werden Innovationen als Geschäftsgeheimnisse behandelt, die dann auch unter das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) fallen. Zukünftig müssten die Unternehmen ihre Arbeitsergebnisse beziehungsweise Geschäftsgeheimnisse sichern, indem sie beispielsweise den Schutz durch eine technische Grenze über die (teilweise) Verschlüsselung von Schnittstellen oder über die Entwicklung einer eigenen Software, die einerseits den gesetzlich geforderten Zugang berücksichtigt, aber andererseits auch den Schutz der Geschäftsgeheimnisse wahrt, gewährleisten. Dies könnte für die betroffenen Unternehmen eine Herausforderung darstellen[31].

[29] u.a. auch VAUNET – Verband privater Medien e.V., EU-Kommission stellt Data Act vor, Beitrag vom 25.02.2022, online abrufbar unter https://www.vau.net/medien-netzpolitik/content/eu-kommission-stellt-data-act, Datum des letzten Abrufs: 01.04.2022; unter Bezugnahme auf einen Artikel in der FAZ vom 20.02.2022.
[30] *Johner*, a.a.O.
[31] siehe hierzu Podszun, a.a.O., S. 66.

mm. Art. 7 Datengesetz – Umfang der Pflichten zur Datenweitergabe von Unternehmen an Verbraucher und zwischen Unternehmen

Gemäß Art. 7 Abs. 1 Datengesetz gelten die ***Pflichten des Kapitels II nicht für Daten, die bei der Nutzung von Produkten oder verbundenen Diensten erzeugt werden, die von Unternehmen hergestellt beziehungsweise erbracht werden, die als Kleinst- oder Kleinunternehmen im Sinne des Art. 2 des Anhangs der Empfehlung 2003/361/EG gelten***, sofern es sich bei diesen nicht um Partnerunternehmen oder verbundene Unternehmen im Sinne der vorgenannten Empfehlung handelt. Die Pflichten betreffen mithin nur Unternehmen, die mehr als 49 Beschäftigte und mehr als 10 Millionen Euro Jahresumsatz/-bilanz haben.

Die Regelung ist aus Sicht der **Clearingstelle** grundsätzlich zu begrüßen, da Kleinst- und Kleinunternehmen regelmäßig nicht über die personellen und finanziellen Ressourcen verfügen, um die statuierten Pflichten zu erfüllen. Sie könnte jedoch insofern problematisch sein, als dass ein solcher Ausschluss auch dazu führen könnte, dass Nutzer sich als Vertragspartner eher Unternehmen aussuchen, denen gegenüber sie ihr Herausgabeverlangen auch rechtlich durchsetzen könnten, was wiederum auch zum Ergebnis haben könnte, dass der Anreiz, Daten selbst zu generieren, um diese für Produktinnovationen zu verwenden, nicht (mehr) gegeben ist. Auf Seiten der Kleinst- und Kleinunternehmen könnte mithin dennoch Druck entstehen, den Pflichten freiwillig nachzukommen, um wettbewerbsfähig bleiben zu können.

c. Kapitel III: Pflichten der Dateninhaber, die rechtlich verpflichtet sind, Daten bereitzustellen

Dem Kapitel III können allgemeine Vorschriften für die Datenbereitstellungspflichten entnommen werden.

aa. Art. 8 Datengesetz – Bedingungen, unter denen Dateninhaber Datenempfängern Daten bereitstellen

Die Bedingungen, unter denen Dateninhaber Datenempfängern Daten bereitstellen, haben ***fair, angemessen und nichtdiskriminierend*** **zu sein** und eine Bereitstellung hat ***in transparenter Weise*** zu erfolgen (Art. 8 Abs. 1 Datengesetz). Hierfür treffen die Parteien eine Vereinbarung, wobei festgelegt wird, dass eine Vertragsklausel in Bezug auf den Datenzugang oder die Haftung und Rechtsbehelfe bei der Verletzung oder Beendigung datenbezogener Pflichten nicht bindend ist, wenn sie die Bedingungen des Art. 13 erfüllt oder wenn sie die Ausübung der Rechte des Nutzers nach Kapitel II ausschließt, davon abweicht oder deren Wirkung abändert (Art. 8 Abs. 2 Datengesetz). Den Parteien soll es ansonsten freistehen, die

genauen Bedingungen für die Bereitstellung von Daten und ihren Verträgen im Rahmen der allgemeinen Zugangsvorschriften für die Bereitstellung von Daten auszuhandeln (Erwägungsgrund 39).

Die Datenbereitstellung darf nicht zwischen vergleichbaren Kategorien von Datenempfängern diskriminierend sein und sollte ein Datenempfänger der Ansicht sein, dass die Bedingungen, unter denen ihm Daten bereitgestellt werden, diskriminierend sind, so obliegt dem Dateninhaber der Nachweis, dass keine Diskriminierung vorliegt (Art. 8 Abs. 3 Datengesetz). Dies stellt eine Beweislastumkehr dar, die für KMU als Nutzer und Datenempfänger grundsätzlich zu begrüßen ist.

Darüber hinaus dürfen einem Datenempfänger gemäß Art. 8 Abs. 4 Datengesetz Daten nur dann exklusiv zur Verfügung gestellt werden, wenn der Nutzer dies gemäß Kapitel II verlangt hat. Ob dies praktikabel und umsetzbar ist, erscheint aus Sicht der **Clearingstelle** zumindest fraglich.

Dateninhaber und Datenempfänger brauchen keine Informationen herauszugeben, die über das hinausgehen, was erforderlich ist, um die Einhaltung der für die Datenbereitstellung vereinbarten Vertragsbedingungen oder die Erfüllung ihrer rechtlichen Pflichten, die sich aus Unionsrechts ergeben, zu überprüfen (Art. 8 Abs. 5). Fraglich ist, ob eine klare Abgrenzung in tatsächlicher Hinsicht durch die Parteien vorgenommen werden kann.

bb. Art. 9 Datengesetz – Gegenleistung für die Bereitstellung von Daten

Art. 9 Abs. 1 Datengesetz sieht vor, dass ***jede Gegenleistung***, die zwischen einem Datenempfänger für die Bereitstellung von Daten vereinbart wird, ***angemessen sein muss***. Sofern der Datenempfänger ein KMU i. S. d. Art. 2 des Anhangs der Empfehlung 2003/361/EG ist[32], darf die vereinbarte Gegenleistung nicht höher sein als die Kosten, die mit der Bereitstellung der Daten für den Datenempfänger unmittelbar zusammenhängen und dem Verlangen zuzurechnen sind (Art. 9 Abs. 3 Datengesetz). Um überprüfen zu können, ob die vorgenannten Anforderungen erfüllt sind, stellt der Dateninhaber dem Datenempfänger nach Art. 9 Abs. 3 Informationen zur Verfügung, denen die Grundlage für die Berechnung der Gegenleistung ***detailliert*** zu entnehmen sind (Art. 9 Abs. 4 Datengesetz).

Diese Regelung soll gemäß Erwägungsgrund 42 dazu dienen, Anreize für weitere Investitionen in die Erzeugung wertvoller Daten zu schaffen, einschließlich Investitionen in einschlägige technische Instrumente. Hierbei soll es nicht um eine Bezahlung der Daten gehen, sondern im Falle von KMU um einen Ausgleich für die Kosten und Investitionen, die für die Bereitstellung der Daten erforderlich sind. KMU sollen vor übermäßigen wirtschaftlichen Belastungen, die es ihnen schwer machen, innovative Geschäftsmodelle zu entwickeln und zu betreiben, geschützt

[32] *Anm. d. Verf.:* Hiernach zählt ein Unternehmen zu den Kleinstunternehmen, kleinen und mittleren Unternehmen, wenn es nicht mehr als 249 Beschäftigte hat und einen Jahresumsatz von höchstens 50 Millionen Euro erwirtschaftet oder eine Bilanzsumme von maximal 43 Millionen Euro aufweist.

werden. Daher sollte die von ihnen zu tragende Gegenleistung für die Bereitstellung von Daten die ***unmittelbaren Kosten der Bereitstellung der Daten*** nicht übersteigen und nicht diskriminierend sein (Erwägungsgrund 44).

LHN weist hierzu darauf hin, dass die Tatsache, dass die Entschädigung bei KMU nicht diejenigen Kosten übersteigen darf, die unmittelbar mit der Bereitstellung der Daten verbunden sind, aus Handwerkssicht positiv zu bewerten ist.

Erwägungsgrund 45 kann entnommen werden, dass es sich bei den unmittelbaren Kosten für die Bereitstellung von Daten um Kosten handelt, die für die Reproduktion, die elektronische Verbreitung und Speicherung für Daten erforderlich sind, nicht aber die Kosten der Datensammlung oder -produktion betreffen. Diesbezüglich wird von der **Clearingstelle** angeregt, dass diese Begriffsbestimmung in Art. 2 Datengesetz oder direkt in die Regelung aufgenommen wird, damit sie unmittelbar zugänglich ist und ohne langes Suchen zur Kenntnis genommen werden kann. Dieser Vorschlag wird auch von **LHN** unterstützt.

Unmittelbare Kosten für die Bereitstellung von Daten sollten zudem auf den Anteil begrenzt werden, der den einzelnen Datenzugangsverlangen zuzurechnen ist, wobei zu berücksichtigen sein soll, dass der Dateninhaber die erforderlichen technischen Schnittstellen oder die erforderliche Software und Netzanbindung dauerhaft einrichten muss. Dabei wird seitens der EU-Kommission die Überlegung zugrunde gelegt, dass langfristige Vereinbarungen zwischen Dateninhabern und Datenempfängern, zum Beispiel über ein Abonnementmodell, die Kosten im Zusammenhang mit der Bereitstellung der Daten im Rahmen regelmäßiger oder wiederholter Transaktionen in einer Geschäftsbeziehung senken könnten (Erwägungsgrund 45).

Welche Anforderungen an die Unterlagen zu stellen sind, mit denen ***„ausreichend detaillierte Informationen für die Berechnung der Gegenleistung“*** zur Verfügung gestellt werden, ist unklar und sollte konkretisiert werden.

Von **UVN** wird hierzu außerdem angeführt, dass der Aufwand für die Bereitstellung von Daten vom Datenempfänger finanziell angemessen entschädigt werden müsse und insbesondere die notwendigen Investitions- oder Projektkosten, die entstehen, damit Daten auch sinnvoll in ihrem Kontext überhaupt von einem Marktteilnehmer zu einem anderen fließen können, sinken müssten. Diese Kosten zur Datenverteilung seien noch unverhältnismäßig hoch.

cc. Art. 10 Datengesetz – Streitbeilegung

Art. 10 Abs. 1 Datengesetz legt fest, dass Dateninhaber und Datenempfänger ***Zugang zu Streitbeilegungsstellen*** erhalten sollen, um Streitigkeiten in Bezug auf die Festlegung fairer, angemessener und nichtdiskriminierender Bedingungen für die Bereitstellung von Daten und die transparente Art und Weise von der Bereitstellung von Daten beizulegen, wobei die ***Entscheidung*** der Streitbeilegungsstelle, die ***spätestens 90 Tage nach Beantragung*** ergehen

soll (Art. 10 Abs. 7 Datengesetz), für die Parteien ***nur dann bindend*** sein soll, ***wenn die Parteien vor Beginn des Streitbeilegungsverfahrens dem bindenden Charakter ausdrücklich zugestimmt haben*** (Art. 10 Abs. 8 Datengesetz).

Mit der alternativen Möglichkeit zur Streitbeilegung soll das ***Vertrauen in die gemeinsame Datennutzung gestärkt*** werden und den Parteien eine ***einfache, schnelle und kostengünstige Lösung bei Uneinigkeit*** angeboten werden (Erwägungsgrund 48).

Den Parteien soll es darüber hinaus unbenommen bleiben, wirksame Rechtsmittel bei einem ***Gericht*** des Mitgliedstaates einzulegen.

Auf die Frage der **Clearingstelle** an die Beiratsmitglieder, ob bekannt sei, ob solche Möglichkeiten grundsätzlich angenommen werden und bei den Unternehmen auf Zuspruch treffen oder eine weitere Stelle zur Streitbeilegung verzichtbar wäre, teilte die **IHKN** mit, dass die Initiative zur Streitbeilegung im Online-Handel von den Unternehmen nicht begrüßt, sondern vielmehr als Belastung empfunden worden sei. Viele Händler würden diese Möglichkeit auch nach fünf Jahren immer noch ausschließen. Daher dürfte davon auszugehen sein, dass auch in diesem Fall keine Teilnahme am Verfahren erfolgen würde. Diese Regelung erscheine aus Sicht von **IHKN** mithin verzichtbar.

dd. Art. 11 Datengesetz – Technische Schutzmaßnahmen und Bestimmungen über die unbefugte Nutzung oder Offenlegung von Daten

Gemäß Art. 11 Abs. 1 Datengesetz kann der Dateninhaber ***geeignete technische Schutzmaßnahmen, einschließlich intelligenter Verträge***, anwenden, um einen unbefugten Zugang zu den Daten zu verhindern und die Einhaltung der datengesetzlichen Bestimmungen zu gewährleisten sowie die für die Datenbereitstellung vereinbarten Vertragsbedingungen sicherzustellen (Art. 11 Abs. 1). Ein intelligenter Vertrag ist gemäß Art. 2 Nr. 16 Datengesetz ***ein in einem elektronischen Vorgangsregistersystem gespeichertes Computerprogramm, bei dem das Ergebnis der Programmausführung in dem elektronischen Vorgangsregister aufgezeichnet wird.***

Ein Datenempfänger muss – sofern der Dateninhaber oder der Nutzer nicht anderes anweist – im Falle von Falschinformationen, Missbrauch, Zweckentfremdung oder sonstigen Verstößen ***unverzüglich die vom Dateninhaber bereitgestellten Daten und alle etwaigen Kopien davon vernichten*** sowie ***das Herstellen, Anbieten, Inverkehrbringen und Verwenden von Waren, abgeleiteten Daten oder Dienstleistungen, die auf den mit Daten erlangten Kenntnissen beruhen, oder das Einführen, Ausführen und Lagern von in diesem Sinne rechtsverletztenden Waren beenden und rechtsverletzende Waren vernichten*** (Art. 11 Abs. 2 Datengesetz). Ein ***Herstellungs- beziehungsweise Verkaufsstopp*** soll jedoch gemäß Art. 11 Abs. 3 Datengesetz dann nicht greifen, wenn dem Dateninhaber durch die Nutzung der Daten ***kein erheblicher Schaden entstanden ist*** oder wenn ein solcher im Hinblick auf die Interessen des Dateninhabers ***unverhältnismäßig*** wäre.

Hier stellt sich aus Sicht der **Clearingstelle** die Frage, ob diese Regelung praktikabel ist, die Pflichten nachvollzogen werden können und ob nicht sogar ein Vernichtungsnachweis erforderlich wäre. Auch die **IHKN** bestätigt, dass nicht ersichtlich sei, wie die Vernichtung sichergestellt werden soll. Hierbei wäre dann auch zu klären, ob es sich ausschließlich um materielle Schäden handelt, oder ob auch immaterielle Schäden geltend gemacht werden können. Zudem sei der Begriff der „Unverhältnismäßigkeit" ein unbestimmter Rechtsbegriff, der zu gewissen Unsicherheiten und unterschiedlichen Bewertungen führen kann, stellt **IHKN** dar.

d. Kapitel IV: Missbräuchliche Klauseln in Bezug auf den Datenzugang und die Datennutzung zwischen Unternehmen

Mit den Bestimmungen in Kapitel IV soll gewährleistet werden, dass ungleiche Verhandlungspositionen der Vertragsparteien bei vertraglichen Vereinbarungen über den Datenzugang nicht ausgenutzt werden[33].

Mit dem Instrument der Missbräuchlichkeitsprüfung soll die schwächere Vertragspartei vor missbräuchlichen Verträgen geschützt und es soll eine gerechtere Verteilung der Wertschöpfung in der Datenwirtschaft gewährleistet werden[34]. Die Verbote unfairer Klauseln sind ähnlich des deutschen AGB-Rechts ausgestaltet[35].

Zudem sollen Mustervertragsbedingungen, die von der Kommission empfohlen werden, Vertragspartner dabei unterstützen, Verträge mit fairen Bedingungen abzuschließen[36].

Konkret sieht Art. 13 Abs. 1 Datengesetz vor, dass eine ***Vertragsklausel*** in Bezug auf den Datenzugang oder die Datennutzung oder die Haftung und Rechtsbehelfe bei Verletzung oder Beendigung datenbezogener Pflichten, die ein Unternehmen einem KMU einseitig auferlegt hat, ***für KMU nicht bindend*** ist, ***wenn sie missbräuchlich ist*** (Art. 13 Abs. 1 Datengesetz). Dies soll gemäß Art. 13 Abs. 2 dann der Fall sein, ***wenn ihre Verwendung gröblich von der guten Geschäftspraxis beim Datenzugang und bei der Datennutzung abweicht und gegen das Verbot von Treu und Glauben und des redlichen Geschäftsverkehrs verstößt***.

In Art. 13 Abs. 3 lit. a – c Datengesetz ist eine ***Liste von Klauseln aufgeführt, die stets als missbräuchlich gelten***. Art. 13 Abs. 4 lit. a – e Datengesetz können die Klauseln entnommen werden***, von denen davon ausgegangen wird, dass sie missbräuchlich sind***. Sofern eine Klausel nicht in einer der beiden Listen aufgeführt wird, findet die ***allgemeine Missbräuchlichkeitsbestimmung*** statt (siehe hierzu Erwägungsgrund 55).

[33] Vorschlag für ein Datengesetz, COM (2022) 68 final, 2022/0047 (COD), a.a.O., S. 18.
[34] Vorschlag für ein Datengesetz, COM (2022) 68 final, 2022/0047 (COD), a.a.O., S. 18f..
[35] *Heynicke/Schönhagen*, KPMG-Law, Mandanten-Information, IT- und Datenschutzrecht, Februar 2022, a.a.O..
[36] Vorschlag für ein Datengesetz, COM (2022) 68 final, 2022/0047 (COD), a.a.O., S. 19 sowie Erwägungsgrund 55.

LHN merkt hierzu an, dass die Liste mit missbräuchlichen Praktiken in die richtige Richtung gehe und im Wesentlichen die Praktiken enthalte, die auch aus Handwerkssicht als unfair benannt wurden. Auch aus der Sicht von **UHN** wird dies als positiv bewertet.

Darüber hinaus sollen gemäß Art. 13 Datengesetz Kriterien für die Ermittlung missbräuchlicher Vertragsklauseln ***nur für diejenigen Bestandteile eines Vertrages gelten, die sich auf die Bereitstellung von Daten beziehen*** (Vertragsklauseln über den Datenzugang und die Datennutzung) sowie die Haftung oder Rechtsbehelfe bei Verletzung und Beendigung datenbezogener Pflichten (Erwägungsgrund 53) und nur auf ***überzogene Vertragsbedingungen***, bei denen eine stärkere Verhandlungsposition missbraucht wird.

Nach Art. 13 Abs. 5 S. 1 Datengesetz soll eine Vertragsklausel nur dann als ***einseitig auferlegt*** gelten, ***wenn sie von einer Vertragspartei eingebracht wird und die andere Partei den Inhalt trotz des Versuchs, hierüber zu verhandeln, nicht beeinflussen kann***. In Erwägungsgrund 52 wird hierzu dargestellt, dass hiermit Situationen gemeint sein sollen, in denen eine Partei eine bestimmte Vertragsklausel einbringt und das KMU den Inhalt der Klausel trotz Verhandlungsversuchs nicht beeinflussen kann und dass eine Vertragsklausel, die lediglich von einer Partei eingebracht und von dem KMU akzeptiert wird oder eine Klausel, die zwischen den Vertragsparteien ausgehandelt und anschließend in geänderter Weise vereinbart wird, nicht als einseitig auferlegt gelten soll.

Dabei soll die Vertragspartei, die eine Vertragsklausel eingebracht hat, die ***Beweislast*** dafür tragen, dass diese Klausel nicht einseitig auferlegt wurde. Aus Sicht von der **IHKN** erscheint diese Regelung nicht praktikabel, da jeder Schrift bei der Vertragsgestaltung und -verhandlung grundsätzlich von der „stärkeren“ Partei dokumentiert werden müsste, was zu einem nicht unerheblichen formalen Aufwand führen würde.

e. Kapitel V: Bereitstellung von Daten für öffentliche Stellen und Organe, Einrichtungen und sonstige Stellen der Union wegen außergewöhnlicher Notwendigkeit

In Kapitel V des Datengesetzes wird festgelegt, dass unter bestimmten Umständen auch öffentlichen Einrichtungen ein erweiterter Zugang zu Daten eingeräumt werden muss. Eine Pflicht zur Bereitstellung ist gemäß Art. 14 Abs. 1 Datengesetz auf Verlangen einer öffentlichen Stelle, einem Organ, einer Einrichtung oder einer sonstigen Stelle der Union dann gegeben, wenn diese eine ***außergewöhnliche Notwendigkeit der Nutzung der verlangten Daten*** nachweist.

Kleine und Kleinstunternehmen werden von dieser Pflicht nach Art. 14 Abs. 2 Datengesetz ausgenommen. Zu diesem Aspekt gibt die **AG KSpV** zu bedenken, dass es in äußersten Notlagen auch von Bedeutung sein könne, Daten derartiger Unternehmen zu erhalten. Dies gelte zum Beispiel für Innovative Start-Ups und andere Firmen, die trotz ihrer fehlenden Größe erforderliche Daten besitzen.

Der Begriff ***„öffentliche Stelle“*** wird in Art. 2 Nr. 9 Datengesetz legal definiert. Hierbei handelt es sich um die nationalen, regionalen und lokalen Behörden, Körperschaften und Einrichtungen des öffentlichen Rechts der Mitgliedstaaten oder Verbände, die aus einer oder mehreren dieser Behörden, Körperschaften oder Einrichtungen bestehen.

Ob ein Unternehmen aus dieser Begriffsbestimmung unmittelbar und ohne weitere Prüfung nachvollziehen kann, dass es der konkret anfragenden öffentlichen Stelle gegenüber zur Bereitstellung von Daten verpflichtet ist, ist zweifelhaft. Aus Sicht der **Clearingstelle** sollte den Unternehmen in jedem Fall diesbezüglich weiterführende Informationen, zum Beispiel eine Liste der öffentlichen Stellen, die wirksam ein Herausgabeverlangen geltend machen können, zur Verfügung gestellt werden. Auch seitens **LHN** wird dies für einen gangbaren Weg gehalten.

Die **AG KSpV** hält dagegen weiterführende Informationen für Unternehmen, wie die vorgeschlagene Liste der öffentlichen Stellen, in den allermeisten Fällen für entbehrlich. Unzweifelhaft dürften die Gebietskörperschaften wie Bund, Länder und Kommunen und alle öffentlich-rechtlichen Einrichtungen unter den Adressatenkreis fallen, der von den Rechten aus Kapitel 5 Gebrauch machen können sollte, so **AG KSpV**. Darüberhinausgehende öffentliche Stellen könnten gegebenenfalls durch mitgliedstaatspezifische Hinweise veröffentlicht werden. Überdies setze Art. 17 Datengesetz voraus, dass die öffentliche Stelle umfassend die Umstände des Datenverlangens darlegt und dies in verständlicher Sprache formuliert. Insofern dürfte das Informationsbedürfnis des Dateninhabers aus Sicht der **AG KSpV** hinreichend berücksichtigt worden sein.

Art. 15 Datengesetz bestimmt, wann eine ***außergewöhnliche Notwendigkeit der Datennutzung*** gegeben ist. Dies ist der Fall, wenn die Daten zur Bewältigung eines öffentlichen Notstands erforderlich sind, ein öffentlicher Notstand verhindert oder bekämpft werden muss oder die öffentliche Stelle ohne die angeforderten Daten nicht ihren rechtlichen Verpflichtungen nachkommen kann.

Aus Sicht der **Clearingstelle** sollten ausschließlich Daten erfragt beziehungsweise angefordert werden, die auch unbedingt für die Bewältigung, Bekämpfung oder Verhinderung eines öffentlichen Notstands erforderlich sind. Informationen, die anderweitig erlangt werden können oder gegebenenfalls bereits bei anderen Behörden vorhanden sind, sollten nicht erneut bei den betroffenen Unternehmen angefordert werden.

Welche Voraussetzungen ein wirksames Datenbereitstellungsverlangen von den öffentlichen Stellen erfüllt werden muss, wird in Art. 17 Datengesetz beschrieben. Insbesondere der Umstand, dass ein Datenverlangen in ***klarer, prägnanter, einfacher und für den Dateninhaber verständlicher Sprache abgefasst sein muss*** (Art. 17 Abs. 2 lit. a Datengesetz) und dass es die ***rechtmäßigen Ziele des Dateninhabers unter Berücksichtigung des Schutzes von Geschäftsgeheimnissen und der Kosten und des nötigen Aufwands der Datenbereitstellung zu achten*** hat (Art. 17 Abs. 2 lit. c), ist aus Sicht von betroffenen (mittleren) Unternehmen zu begrüßen, was auch von **LHN** ausdrücklich bestätigt wird.

Gemäß Art. 18 Abs. 1 Datengesetz hat ein Dateninhaber, der ein Datenzugangsverlangen erhält, der anfragenden öffentlichen Stelle die Daten ***unverzüglich*** bereit zu stellen. ***Ausnahmen*** hiervon werden in Art. 18 Abs. 2 Datengesetz aufgeführt, nach dem der Dateninhaber dann, ***wenn die angeforderten Daten nicht verfügbar sind oder das Verlangen nicht die in Art. 17 Abs. 1 und 2 festgelegten Voraussetzungen erfüllt***, in Fällen eines ***öffentlichen Notstands binnen 5 Arbeitstagen*** und ***in anderen Fällen einer außergewöhnlichen Notwendigkeit binnen 15 Arbeitstagen*** das Verlangen ***ablehnen*** oder eine Änderung desselben beantragen kann.

Eine ***Ablehnung*** ist gemäß Art. 18 Abs. 3 Datengesetz auch möglich, wenn der Dateninhaber die verlangten Daten bereits auf ein vorheriges Verlangen einer ***anderen öffentlichen Stelle zur Verfügung gestellt*** hat. In diesem Fall hat er die Stelle, der er die verlangten Daten zu demselben Zweck übermittelt hat, zu benennen. Auch hier sollte erst in einem zweiten Schritt das dateninhabende Unternehmen verpflichtet werden. Die Koordinierung von Auskunftsverlangen sollte aus Sicht der **Clearingstelle** daher nur in Ausnahmefällen den betroffenen Unternehmen aufgebürdet werden und die behördlichen Stellen sollten zunächst untereinander in Erfahrung bringen, ob ein Austausch der relevanten Informationen möglich ist.

Die **IHKN** gibt hierzu jedoch zu bedenken, dass Daten, wenn diese dann von einer behördlichen Stelle bei einer anderen behördlichen Stelle angefragt werden und diese von dort übermittelt werden müssten, bei den Behörden gegebenenfalls auch über den eigentlich verfolgten Zweck hinaus gespeichert werden müssten. Zudem bestünde gemäß **IHKN** die Gefahr einer intransparenten „Datenkette“. Im Falle eines Missbrauchs könnten Fehlerquellen laut **IHKN** dann nur schwer nachzuvollziehen sein.

Die **AG KSpV** merkt an, dass die Einschätzung der **Clearingstelle** bezüglich des Koordinationsaufwands für Unternehmen ausdrücklich nicht geteilt werde und im Falle eines eilbedürftigen Notstandes eine Abfrage unter verschiedenen Stellen nicht abgewartet werden dürfe. Die sich aus Art. 18 Abs. 4 Datengesetz ergebende Hinweispflicht des Dateninhabers an die zuvor anfragende öffentliche Stelle stelle aus Sicht der **AG KSpV** keinen unzumutbaren Aufwand für Unternehmen dar.

Bei der Erfüllung des Datenzugangsverlangens hat der Dateninhaber die ***Daten*** zu ***pseudonymisieren***, sofern es sich um ***personenbezogene Daten*** handelt ***und das Verlangen mit pseudonymisierten Daten erfüllt werden kann***. Personenbezogene Daten sind für das Handwerk zum Beispiel insbesondere bei individuellen Kundenaufträgen und in der Kommunikation mit Kunden von Belang[37]. Mit der Pseudonymisierung können Daten geschützt werden, indem die Werte von direkten Identifikatoren (zum Beispiel Namen, Ausweisnummern) durch Pseudonyme ersetzt werden, die aus dem ursprünglichen Wert erzeugt oder neu vergeben werden. Die Zuordnung muss hierbei immer eindeutig sein, um

[37] *Podszun*, a.a.O., S. 38.

eine Umkehrung zu gewährleisten, welche immer dann möglich ist, wenn aus dem erzeugten Pseudonym der ursprüngliche Datenwert abgeleitet werden kann[38].

In Notstandsituationen sind die Daten unentgeltlich bereitzustellen (Art. 20 Abs. 1), in anderen Fällen kann der Dateninhaber einen Ausgleich verlangen, der jedoch nicht die ***technischen oder organisatorischen Kosten, die durch die Erfüllung des Verlangens*** entstehen, erforderlichenfalls einschließlich der Kosten einer Anonymisierung und technischen Anpassung, zuzüglich einer ***angemessenen Marge***, übersteigen dürfen. Im Zweifel sind die Grundlagen für die Berechnung der Kosten sowie der angemessenen Marge der öffentlichen Stelle zu übermitteln.

Da Unternehmen in unterschiedlichster Form Aufgaben für den Staat erledigen müssen, die ihnen per Gesetz oder Verordnung auferlegt werden, wirkt dies für diese oftmals – insbesondere dann, wenn sie unentgeltlich erbracht werden – wie eine „Überwalzung von Bürokratie". Aus diesem Grund wird vielfach gefordert, dass bei staatlichen Auskunftspflichten ein Kostenerstattungsprinzip gelten müsse, mit welchem zum einen Anreize gesetzt werden könnten, Informationspflichten auf ein notwendiges Maß zu beschränken (Abwägung von Kosten und Nutzen durch den Staat, siehe auch Art. 17 Abs. 2 lit. c Datengesetz) und zum anderen die Akzeptanz bei Unternehmen durch eine finanzielle Entlastung zu stärken[39]. Es ist daher aus Sicht der **Clearingstelle** zu begrüßen, dass eine Kostenerstattung beabsichtigt ist. Gleichwohl erscheint es sinnvoll, wenn hier weitere Einzelheiten – gegebenenfalls über einen Katalog mit möglichen Daten, die in bestimmten Fällen angefordert werden könnten und den entsprechenden erstattungsfähigen Kosten (am besten in Form von Pauschalen)[40] – festgelegt werden, um Transparenz zu schaffen und weitere Bürokratie zu vermeiden, die insbesondere dann entstehen könnte, wenn im Einzelfall die Frage zu klären ist, ob eine „angemessene Marge" vom Dateninhaber veranschlagt wurde.

Auch die **AG KSpV** gibt zu bedenken, dass unklar sei, was eine angemessene Marge darstellt. Naturgemäß sollte die Formulierung daher allen Einzelfällen in Abhängigkeit vom tatsächlichen Personal- und Sachaufwand gerecht werden, so **AG KSpV**. Dennoch würden auch aus Sicht der **AG KSpV** Orientierungswerte, zum Beispiel in den später zu erwartenden delegierten Rechtsakten, eine Hilfestellung bieten.

[38] Bitkom - Bundeverband Informationswirtschaft, Telekommunikation und neue Medien e.V., Anonymisierung und Pseudonymisierung von Daten für Projekte des maschinellen Lernens, eine Handreichung für Unternehmen, Berlin 2020, S. 5 f., online abrufbar unter https://www.bitkom.org/sites/default/files/2020-10/201002_lf_anonymisierung-und-pseudonymisierung-von-daten.pdf, Datum des letzten Abrufs: 05.04.2020.
[39] *Kroker/Lichtblau/Röhl,* Abbau von Bürokratie in Deutschland: Mehr als die Abschaffung von Einzelvorschriften, IW-Analysen, Nr. 3, Institut der Deutschen Wirtschaft (IW), Köln, 2004, S. 124f..
[40] *Kroker/Lichtblau/Röhl*, S. 125f..

f. Kapitel VI: Wechsel zwischen Datenverarbeitungsdiensten

In Kapitel VI werden Regelungen festgelegt, die zukünftig den Kundinnen und Kunden von Anbietern von Datenverarbeitungsdiensten den Wechsel zwischen diesen erleichtern sollen. Da KMU nicht nur Nutzer/Kunden, sondern auch selbst Anbieter von Datenverarbeitungsdiensten sein können, und diesen durch dieses und die folgenden Kapitel VII und VIII zusätzliche Verpflichtungen auferlegt werden, geht die **Clearingstelle** diesbezüglich auf ausgewählte Aspekte detaillierter ein.

Gemäß Artikel 24 Datengesetz müssen die ***Rechte des Kunden und die Pflichten des Anbieters eines Datenverarbeitungsdienstes*** in Bezug auf den Wechsel zwischen Anbietern solcher Dienste in einem schriftlichen Vertrag eindeutig festgelegt werden. Unter anderem muss dieser Vertrag mindestens Klauseln enthalten, die es dem Kunden ermöglichen, auf Verlangen zu einem Datenverarbeitungsdienst zu wechseln, der von einem anderen Anbieter von Datenverarbeitungsdiensten angeboten wird, oder alle direkt oder indirekt vom Kunden erzeugten Daten, Anwendungen und digitalen Vermögenswerte auf ein System in eigenen Räumlichkeiten zu übertragen (Art. 24 Abs. 1 lit. a Datengesetz). Die stellt in jedem Fall eine zusätzliche bürokratische Last für betreffenden Unternehmen dar. Ob es für diese ohne Weiteres möglich ist, zu identifizieren, welche Daten indirekt von den Kunden erzeugt wurden und ob diese auch ohne größeren Aufwand den Kunden zur Verfügung gestellt werden können, erscheint fraglich.

In Art. 24 Abs. 2 wird auf die verbindliche Übergangsfrist von 30 Kalendertagen hingewiesen und erläutert, wie verfahren werden soll, wenn diese technisch für den Anbieter nicht machbar sein sollte. Diese Einzelheiten müssen dem Kunden vom Anbieter des Datenverarbeitungsdienstes innerhalb von sieben Arbeitstagen nach der Veranlassung des Anbieterwechsels mitgeteilt werden, wobei der Anbieter die technische Undurchführbarkeit mit einem ausführlichen Bericht ordnungsgemäß begründen und einen alternativen Übergangszeitraum angeben muss. Die **Clearingstelle** möchte in diesem Zusammenhang darauf hinweisen, dass nicht ersichtlich ist, welche Form und welchen Umfang der „ausführliche Bericht“ haben muss. Hiervon positive Kenntnis zu erlangen, erfordert weiteren Aufwand bei den von der Regelung betroffenen Unternehmen.

g. Kapitel VII: Schutzvorkehrungen für nicht personenbezogene Daten

Kapitel VII behandelt den unrechtmäßigen Zugang Dritter zu nicht personenbezogenen Daten, die in der Union im Besitz von auf dem Unionsmarkt angebotenen Datenverarbeitungsdiensten sind. Gemäß Art. 27 Abs. 1 müssen die Anbieter von Datenverarbeitungsdiensten alle ***angemessenen technischen, rechtlichen und organisatorischen Maßnahmen*** treffen, ***einschließlich vertraglicher Vereinbarungen***, um eine internationale Übermittlung oder einen internationalen Zugriff zu in der Union

gespeicherten nicht personenbezogenen Daten zu verhindern, wenn dies im Widerspruch zum Unionsrecht oder zum nationalen Recht des betreffenden Mitgliedstaats stünde. Welche konkreten rechtlichen Maßnahmen die Anbieter von Datenverarbeitungsdiensten ergreifen müssen, bleibt aus Sicht der **Clearingstelle** unklar. Dies ***gilt auch für die Frage, ob KMU diese Anforderungen überhaupt ohne Weiteres leisten können oder hierfür fremde Beratungsleistungen in Anspruch nehmen müssen***. In beidem Fall entsteht zumindest zeitlicher Aufwand.

Aus Art. 27 Absatz 4 geht hervor, dass der Anbieter von Datenverarbeitungsdiensten, aufgrund einer angemessenen Auslegung des Verlangens die zulässige Mindestmenge der darin verlangten Daten bereitstellen soll, falls die Voraussetzungen des Absatzes 2 oder 3 erfüllt sind. Es stellt sich hier unter anderem die Frage, ob die Anbieter von Datenverarbeitungsdiensten bei der Prüfung der in den Absätzen 2 und 3 genannten Voraussetzungen unterstützt werden oder ob die Prüfung beziehungsweise Recherche der Einzelheiten lediglich durch die Anbieter selbst erbracht werden muss. ***Hier sollte geprüft werden, ob es nicht eine Möglichkeit gibt, die Anbieter von Datenverarbeitungsdiensten entsprechend zu entlasten***. Zudem entstehen den Unternehmen durch das Bereitstellen der Daten voraussichtlich zeitliche Aufwände, die nicht vergütet werden.

h. Kapitel VIII: Interoperabilität

Anbieter von Datenverarbeitungsdiensten sollen verpflichtet werden, die Interoperabilität durch offene Standards und Schnittstellen zu erleichtern. Nach den Begriffsdefinitionen in Artikel 2 Nr. 19 des Datengesetzes wird „Interoperabilität“ als die Fähigkeit von zwei oder mehr Datenräumen oder Kommunikationsnetzten, Systemen, Produkten, Anwendungen oder Komponenten, beschrieben, Daten auszutauschen und zu verwenden, um ihre Funktionen auszuführen. Aus den in Art. 28 Abs. 1 aufgelisteten wesentlichen Anforderungen an die Interoperabilität, ergeben sich im Zuge der Erfüllung dieser auch zeitliche Aufwände für die Betreiber von Datenräumen.

Nichtsdestotrotz sollte nach Auffassung der **Clearingstelle** berücksichtigt werden, dass sich teilweise Zugangsprobleme gar nicht erst stellen, wenn es keine technischen Einschränkungen beim Zugang geben würde. Durch offene Schnittstellen, frei zugängliche Formate oder Standardisierungen könnte das Ausschließungspotenzial letztlich verringert[41] und technische Barrieren reduziert werden[42]. Sofern zum Beispiel alle Smart Homes mit einer gleichartigen, standardisierten Software gesteuert werden könnten, würde dies allen Handwerkern den Zugang zu diesem Smart Home erleichtern, ohne dass zunächst Lizenzverträge mit dem Operator geschlossen werden müssten. Die Einigung auf einen Standard könnte auch zur Folge haben, dass zwischen Anbietern verschiedener Lösungen ein Wettbewerb um die besten

[41] *Podszun*, a.a.O., S. 127.
[42] *Podszun*, a.a.O., S. 128f..

Anwendungen im Smart Home entsteht[43]. Durch die ***Verpflichtung der Anbieter bestimmte Standards und Schnittstellen einzurichten***, wird es den Unternehmen (in diesem Fall direkten Kunden oder Dritten) ermöglicht, mit eigenen „Werkzeugen" an das System anzudocken[44].

Da die Entwicklung interoperabler Formate und Standards typischerweise nicht in den Händen eines hoheitlichen Gesetzgebers liegt, sondern weitestgehend der Selbstregulierung der Industrie überlassen und vom Gesetzgeber nur für verbindlich erklärt wird, sollte es essentiell sein, dass bei stattfindenden Aushandlungsprozessen Vertreter aller zukünftig betroffenen Gruppen beteiligt werden[45]. Initiativen, in denen allein Gatekeeper vertreten sind, werden keine Lösungen finden, die spezifische Interessen von kleinen Unternehmen berücksichtigen. Beispielsweise kommt es für Handwerksunternehmen darauf an, dass die Lösungen auch für KMU einfach zugänglich sind, dass Reparatur- und Wartungsfragen von vornherein berücksichtigt werden, dass kein hoher bürokratischer Aufwand durch Registrierung, Dokumentation oder ähnliches entsteht, den sich kleinere Unternehmen nicht erlauben oder dass individuelle Materiallösungen berücksichtigt werden können[46].

i. Kapitel IX: Anwendung und Durchsetzung

Jeder Mitgliedstaat hat ***eine oder mehrere zuständige Behörden zu benennen***, die für die Anwendung und Durchsetzung des Datengesetzes verantwortlich sind, wobei neue Behörden eingerichtet oder bestehende Behörden genutzt werden können (Art. 31 Abs. 1 Datengesetz).

Da aus Art. 31 Abs. 2 Datengesetz ersichtlich wird, dass hier Überschneidungen beziehungsweise Abgrenzungszuständigkeiten zwischen verschiedenen Aufsichtsbehörden beziehungsweise Zuständigkeiten gegeben sein könnten, sollte es nach Ansicht der **Clearingstelle** den Betroffenen so einfach wie möglich gemacht werden, herauszufinden, welche Behörde für welche Fälle beziehungsweise für welche Anliegen zuständig ist. Auch sollte sichergestellt werden, dass die (Fach-)Behörden untereinander Sachverhalte weiterverweisen können, damit die betroffenen Unternehmen nicht von einer Stelle zu nächsten geschickt werden. Dies sollte durch das (frühzeitige) Einholen von entsprechenden Einverständniserklärungen unter Aufklärung über etwaige Rechte und Pflichten der Betroffenen sichergestellt werden.

Als erfreulich ist die Regelung in Art. 31 Abs. 3 Datengesetz, nach welcher die zuständige Behörde auch dazu ***verpflichtet wird, technische Entwicklungen zu beobachten***, die für die Bereitstellung und Nutzung von Daten von Bedeutung sind (Art. 31 Abs. 3 lit. e Datengesetz) sowie dazu, mit den zuständigen Behörden anderer Mitgliedstaaten zusammenzuarbeiten (Art. 31 Abs. 3 lit. f Datengesetz), anzusehen. Dies könnte dazu führen, dass auf relevante

[43] *Podszun*, a.a.O., S. 128f..
[44] *Podszun*, a.a.O., S. 127.
[45] *Podszun*, a.a.O., S. 130.
[46] Ebenda.

Veränderungen in den betroffenen Bereichen bzw. auf den betroffenen Märkten frühzeitig und adäquat reagiert werden kann.

Gemäß Art. 33 Abs. 1 Datengesetz erlassen die Mitgliedstaaten ***Sanktionen, die bei Verstößen gegen das Datengesetz zu verhängen sind*** und treffen die für ihre Anwendung erforderlichen Maßnahmen. Diese müssen wirksam, verhältnismäßig und abschreckend sein. Verstöße gegen die Pflichten aus Kapitel II, III und V des Datengesetzes sollen sich dabei nach den Vorgaben der DSGVO richten (Art. 33 Abs. 3 Datengesetz), so dass potentiell Geldbußen bis zu 20.000.000 Euro beziehungsweise 4 % des weltweit erzielten Jahresumsatzes des vorausgegangenen Geschäftsjahres verhängt werden können. Hier könnte ***in Erwägung gezogen werden, die Erfahrungen von Unternehmen mit der Verhängung von Geldbußen aufgrund der DSGVO heranzuziehen***, um zu beurteilen, ob die abschreckende Wirkung der Sanktionen auch greift und die entsprechende Regelung sinnvoll und zielgerichtet ist[47].

Art. 34 Datengesetz sieht vor, dass die Kommission ***unverbindliche Mustervertragsbedingungen für den Datenzugang und die Datennutzung*** erstellen und empfehlen wird, um die Parteien bei der Aushandlung von Verträgen mit ausgewogenen vertraglichen Rechten und Pflichten zu unterstützen. Dies ist aus Sicht von KMU zu begrüßen, da sie so vertragliche Regelungen einsehen und sich an diesen orientieren können, sofern sie selbst ohne fremde rechtliche Expertise Verträge verhandeln oder erstellen möchten, um Kosten zu sparen[48]. In diesem Zusammenhang sollte in Erwägung gezogen werden, ***branchenspezifische Vertragsmuster*** vorzubereiten und den Unternehmen zur Verfügung zu stellen[49].

Auch sollten in diesem Zusammenhang Hinweise zur Möglichkeit der Ausgestaltung der Verträge mit Vertragsstraferegelungen aufgeführt werden, mit welchen Verletzungen gegen die Pflichten aus dem Datengesetz auch zivilrechtlich sanktioniert werden könnten. Wie an anderer Stelle bereits erwähnt, erscheinen die Anforderungen an den zu erbringenden Nachweis für einen kausalen Schaden im Zusammenhang mit der Zurverfügungstellung von Daten zu hoch und die allgemeinen Regelungen des Schadensersatzrechtes als ungeeignet, um den nötigen Sanktionsmöglichkeiten für Pflichtverletzungen Genüge tun zu können[50].

Ferner könnten auch in diesen Vertragsbedingungen konkrete Modalitäten für die Bereitstellung der Daten (zum Beispiel, welches Format, welche Aktualität des Formats, einzuhaltender Standard in Bezug auf die Sicherheit, etc.) aufgeführt werden[51]. Nur so kann ein Vertragspartner, der auf ein ganz anderes Themengebiet spezialisiert ist (zum Beispiel der Inhaber einer Kfz-Werkstatt) auch angemessen ***nachvollziehen, ob der Dateninhaber seiner Pflicht zur Zugänglichmachung der Daten auch adäquat nachgekommen ist***.

[47] *Anm. d. Verf.:* Dies war der Clearingstelle binnen der Frist zur Abgabe der Stellungnahme leider nicht möglich.
[48] siehe hierzu auch *Podszun*, a.a.O., S. 148.
[49] *Podszun*, a.a.O., S. 9.
[50] siehe hierzu auch *Podzun*, a.a.O., S. 139.
[51] *Podszun*, a.a.O. S. 149.

Es sollte jedoch aus Sicht der **Clearingstelle** sichergestellt sein, dass ***diese Mustervertragsbedingungen auch rechtzeitig vorliegen*** und nicht erst während oder nach Ablauf der Übergangsfrist (siehe unten) veröffentlicht werden.

Die Verordnung soll ***zwölf Monate nach dem Datum des Inkrafttretens gelten*** (Art. 42 Datengesetz), so dass den Unternehmen zumindest eine Übergangsfrist zur Überarbeitung der Produkte, Produktunterlagen, Vertragsbedingungen, etc. eingeräumt wird.

Zudem soll das Datengesetz ***binnen zwei Jahren nach Geltungsbeginn evaluiert werden*** (Art. 41 Abs. Datengesetz), was ausdrücklich zu begrüßen ist. In diesem Zusammenhang ist aus Sicht der Clearingstelle jedoch darauf zu achten, dass bei einer Bewertung des Datengesetzes die Expertise unterschiedlicher Akteure und Institutionen herangezogen wird[52], damit auch in diesem Zusammenhang (mittelbare) bürokratische Lasten für KMU unterschiedlicher Branchen erkannt, benannt sowie bewertet und bei auftretenden Problemen schnelle und lösungsorientierte Möglichkeiten zur Abhilfe geschaffen werden können.

IV. Votum

Die **Clearingstelle** hat den Entwurf des Datengesetzes im Rahmen einer beratenden Stellungnahme gemäß § 31a Abs. 2 S. 3 GGO dahingehend geprüft, ob die darin enthaltenen Regelungen und die vorgesehenen Mechanismen zur Ermöglichung von Datenaustausch für KMU umsetzbar und nutzbar sind. Insbesondere wurde der Entwurf auf bürokratische Lasten untersucht und – sofern im Einzelfall möglich – bürokratieärmere Regelungen beziehungsweise Vorgehensweisen benannt. Folgende Aspekte des Data Acts sind aus Sicht der **Clearingstelle** insbesondere erwähnenswert und/oder verbesserungswürdig:

- **Kapitel I, Art. 2 Datengesetz**
  Der Umstand, dass in Art. 2 Nr. 1 bis 20 Datengesetz die wesentlichen Begriffe definiert werden, wird begrüßt, da so möglich ist, die Rechte und Pflichten der Betroffenen nachzuvollziehen. Gleichwohl sollten ***hier weitere Definitionen aufgenommen sowie eine nachvollziehbare Abgrenzung zwischen personenbezogenen und nicht personenbezogenen Daten*** sowie eine Festlegung der diesbezüglichen konkreten Pflichten vorgenommen werden.

  Die Definition in ***Art. 2 Nr. 5 Datengesetz*** *sollte* ***überarbeitet*** beziehungsweise die deutschsprachige Übersetzung nachgebessert werden (siehe hierzu Abschnitt III. 2. b.).

[52] siehe hierzu auch Gutachten des Normenkontrollrates zur Durchführung von Ex-post-Evaluierungen – Gute Praktiken und Erfahrungen des Normenkontrollrates in anderen Staaten, 2013, online abrufbar unter https://www.normenkontrollrat.bund.de/resource/blob/72494/444152/a50b2b0987ab4865b514116498d73ba2/2014-02-11-evaluierungsstudie-data.pdf, Datum des letzten Abrufs: 01.04.2022.

- **Kapitel II, Art. 3 Abs. 1 Datengesetz**
  Mit der Regelung in Art. 3 Abs. 1 Datengesetz scheint nicht gewährleistet zu sein, dass die Hersteller als Dateninhaber rechtssicher ihrer Pflicht zur Zugänglichmachung von Daten nachkommen können. Um Rechtsunsicherheiten zu vermeiden, die vor allem auch aus unbestimmten Rechtsbegriffen resultieren können, sollten – sofern eine Konkretisierung im Einzelfall nicht möglich ist – den betroffenen Unternehmen zumindest ***schnell auffindbare, rechtsverbindliche Erläuterungen*** zur Verfügung gestellt werden. Insbesondere sollte es dem Datengesetz entnommen werden können, was genau mit „Zugang zu Daten" gemeint ist und unter welchen Voraussetzungen und zu welchen Bereichen dieser Zugang zu ermöglichen ist. Die Regelungen sollten unter Berücksichtigung des Zwecks des Datenzugangs erstellt werden und auch die Form und Bedingungen für die Bereitstellung der Daten regeln.

- **Kapitel II, Art. 3 Abs. 2 Datengesetz**
  Auch aus den ***vorvertraglichen Informations- und Transparenzpflichten*** ergeben sich zusätzliche Aufwände für die betroffenen Unternehmen und es kann davon ausgegangen werden, dass hier externe Expertise in Anspruch genommen werden muss. Zudem sollte geprüft werden, inwiefern es sinnvoll ist, Nutzern eine weitere Anlaufstelle für Beschwerden zu benennen und ob eine solche nicht weitere Belastungen und Rechtsunsicherheiten schaffen könnte.

- **Kapitel II, Art. 4 Datengesetz**
  Auch die Regelung in ***Art. 4 Abs. 1 Datengesetz*** wird voraussichtlich zu ***Rechtsunsicherheiten*** führen, da für Unternehmen kaum nachvollziehbar sein wird, wie dem Recht der Nutzer auf Zugang genüge getan werden kann. Zudem bleibt unklar, welche Anforderungen an die Nutzeridentifizierung genau zu stellen sind, so dass eine ***Konkretisierung des Art. 4 Abs. 2 Datengesetz*** angeregt wird. Ferner dürften auch die Anforderungen des ***Art. 4 Abs. 3 Datengesetz*** jedes betroffene Unternehmen, insbesondere auch KMU als Nutzer, überfordern. Hier könnten unter Umständen ***Musterklauseln*** einen Ansatz für eine praktikable Lösung darstellen, in jedem Fall ist jedoch eine klare, praktisch handhabbare ***Definition des „schützenswerten Geschäftsgeheimnisses"*** erforderlich. Auch sollten ***weitere Ausführungen/Konkretisierungen*** in Bezug auf die ***Form einer Vereinbarung*** zwischen Dateninhaber und Nutzer erfolgen.

  Um datenschutzrechtliche Verwerfungen von vorneherein zu vermeiden, sollten ***personenbezogene Daten nach Möglichkeit aus dem Regelungsbereich des Datengesetzes herausgenommen werden*** (***Art. 4 Abs. 5 Datengesetz***). Im Hinblick auf ***nicht personenbezogene Daten*** ist die Regelung in ***Art. 4 Abs. 6 Datengesetz nicht eindeutig genug und nicht praktikabel***, da nicht ersichtlich ist, wie bzw. woran die Parteien erkennen sollen, dass die Daten nicht personenbezogen sind. Hier kann insbesondere auch davon ausgegangen werden, dass Fachkenntnisse Dritter in Anspruch genommen werden müssen, um die vertraglichen Regelungen nachvollziehen zu können.

- **Kapitel II, Art. 5 Datengesetz**
  Obwohl das Recht auf Weitergabe der Daten an Dritte nach ***Art. 5 Abs. 1 Datengesetz*** positiv bewertet wird, wird dieses aber zum Ergebnis haben, dass die ***Anforderungen an die IT-Sicherheit signifikant steigen*** werden. Dieser Umstand führt wiederum zu ***mehr Aufwand, insbesondere auch Kosten***, bei den betroffenen Unternehmen.

  Hinsichtlich ***Art. 5 Abs. 2 Datengesetz*** ist zu berücksichtigen, dass die ***„Gatekeeper"-Eigenschaft*** wohl nicht immer unmittelbar von den Nutzern erkannt werden kann. Hier sollten Maßnahmen ergriffen werden, die es den Nutzern ermöglichen, eine ***schnelle Identifizierung*** der „Gatekeeper" durchzuführen, wobei im Sinne dieser sichergestellt sein sollte, dass keine öffentliche Stigmatisierung mit weiteren nachteiligen Folgen für diese drohen.

- **Kapitel II, Art. 7 Datengesetz**
  Der Umstand, dass ***Kleinst- und Kleinunternehmen von Pflichten des Kapitels II des Datengesetzes ausgenommen werden***, ist grundsätzlich zu begrüßen.

- **Kapitel III, Art. 9 Datengesetz**
  Diesbezüglich wird angeregt, dass die ***Definition, wann eine Gegenleistung als angemessen gilt***, in das Datengesetz aufgenommen wird. Außerdem sollte konkretisiert werden (gegebenenfalls auch über einen Leitfaden), welche Anforderungen an die Unterlagen zu stellen sind, mit denen ***„ausreichend detaillierte Informationen für die Berechnung der Gegenleistung"*** zur Verfügung gestellt werden.

- **Kapitel III, Art. 10 Datengesetz**
  Es sollte noch einmal eine Prüfung angeregt werden, ob es vorliegend ***tatsächlich erforderlich und praktikabel*** ist, ***Streitbeilegungsstellen einzurichten***.

- **Kapitel IV, Art. 13 Datengesetz**
  Wenngleich die ***Regelung*** aus Sicht der Kleinstunternehmen und kleinen Unternehmen ***positiv*** zu bewerten ist, bringt sie für den „stärkeren Vertragspartner", bei dem es sich auch um ein mittleres Unternehmen handeln kann, insbesondere aufgrund der Beweislastumkehr, ***Aufwände*** mit sich.

- **Kapitel V, Art 14 ff. Datengesetz**
  Hier sollte in Erwägung gezogen werden, ob den betroffenen Unternehmen eine ***Liste*** mit den öffentlichen Stellen, die wirksam Auskunftsverlangen geltend machen können, zur Verfügung gestellt wird. Außerdem sollten möglichst auch ***nur Daten*** erfragt beziehungsweise angefordert werden, ***die auch unbedingt erforderlich sind***. Insbesondere sollten Informationen, die auch anderweitig erlangt werden können oder bereits bei Behörden vorhanden sind, möglichst ***ohne Unterstützung der Unternehmen eingeholt werden***.

Zu begrüßen ist, dass grundsätzlich auch eine ***Kostenerstattung*** beabsichtigt ist (Art. 20 Datengesetz). Hier wäre es wünschenswert, wenn ***Orientierungswerte oder Kostenpauschalen*** erarbeitet und festgelegt werden, die den Beteiligten die ***Berechnungsmodalitäten erleichtern***.

- **Kapitel VIII, Art. 28 ff. Datengesetz**
  Die Verbesserungen beziehungsweise Anforderungen hinsichtlich der Erleichterung der Interoperabilität sind grundsätzlich positiv zu bewerten, es gilt jedoch ***einige Aspekte zu berücksichtigen, damit die erstrebenswerten Standardisierungen einen Gewinn für die betroffenen Unternehmen darstellen***.

- **Kapitel IX, Art. 34 Datengesetz**
  Das Vorhaben der Kommission, unverbindliche ***Mustervertragsbedingungen*** für den Datenzugang und die Datennutzung zu erstellen und zu empfehlen, ist positiv zu bewerten. Eine Verbesserungsmöglichkeit könnten gegebenenfalls eine ***verbindliche Empfehlung*** sowie eine ***Vorbereitung branchenspezifischer Vertragsmuster*** darstellen.

Insgesamt ist das mit dem Data Act verbundene Ansinnen, technische Zugangshindernisse weitestgehend auszuschließen, aus Sicht der betroffenen KMU ***positiv zu beurteilen***. Im Data Act-Entwurf befinden sich jedoch eine ***Vielzahl an Pflichten*** für Unternehmen, ***die geeignet sind***, ***erhebliche Aufwände*** bei diesen ***entstehen zu lassen***. Dies gilt insbesondere auch für die ***Gestaltung von Produkten und Dienstleistungen***. Auch sollte berücksichtigt werden, dass lediglich die Pflichten des Kapitels II nicht für Daten, die bei der Nutzung von Produkten oder verbundenen Dienstleistungen erzeugt werden, die von Kleinst- und Kleinunternehmen stammen, gelten. Viele der sonstigen Pflichten, bei denen noch vieles unklar und erörterungsbedürftig ist und die sich auch aufgrund einer Nutzereigenschaft ergeben können, haben mithin ***auch auf KMU Auswirkungen***, ***die sektor- und branchenübergreifend sind***. Hier gibt es aus Sicht der **Clearingstelle** noch ***erheblichen Verbesserungsbedarf***. Bei einer Überarbeitung der Regelungen des Data Acts sollte insbesondere auch die Frage geklärt werden, ***wie Geschäftsgeheimnisse*** konkret ***geschützt werden können*** und ***welche Informationen schützenswert*** sein sollen.