

# Die Vereinbarkeit von Data Trusts mit der Datenschutz- grundverordnung (DSGVO)

Dr. Michael Funke, JBB Rechtsanwälte



Im Auftrag von



gefördert von der



## Fragestellung und Aufbau

Gegenstand dieses Kurzgutachtens ist die Frage, ob und, falls ja, in welcher Form sog. „Data Trusts“ mit dem geltenden Datenschutzrecht, insbesondere der DSGVO, vereinbar sind und – soweit dies nicht der Fall ist – welche Änderungen im Datenschutzrecht erforderlich wären, um Data Trusts zu ermöglichen.

Das Gutachten hat zur Klärung der Frage den folgenden Aufbau:

Zunächst wird beleuchtet, was unter einem Data Trust zu verstehen ist (*B. Was ist ein Data Trust?*),

um den Sachverhalt abzuklären und die Punkte zu identifizieren, welche für eine datenschutzrechtliche Beurteilung des Sachverhalts relevant sind. In einem zweiten Schritt (*C. Können Data Trusts unter der DSGVO datenschutzkonform handeln*) wird dann begutachtet, ob und in welcher Form Data Trusts unter der DSGVO verwirklicht werden können. Schließlich, soweit dies nicht oder nicht vollständig der Fall ist, werden abschließend (*D. Mögliche gesetzgeberische oder behördliche Maßnahmen, um die Situation zu verbessern*) Möglichkeiten erörtert, welche gesetzlichen Änderungen die Schaffung eines Data Trusts ermöglichen oder begünstigen würden.

# Inhalt

<b>A. Executive Summary</b> .....	<b>4</b>
<b>B. Was ist ein Data Trust?</b> .....	<b>6</b>
<b>I. Was ist ein Trust und welche Rechtsbeziehungen bestehen in ihm?</b> .....	<b>6</b>
1. Grundaufbau des Trusts .....	<b>6</b>
2. Rechtliche Konsequenzen der Einrichtung eines Trusts .....	<b>7</b>
3. Zusammenfassung .....	<b>8</b>
<b>II. Was ist ein Data Trust?</b> .....	<b>8</b>
1. Die Grundidee des Data Trusts .....	<b>8</b>
2. Verschiedene rechtliche Formen zur Konstruktion eines Data Trusts .....	<b>9</b>
<b>III. Datenschutzrechtliche Problempunkte</b> .....	<b>10</b>
<b>C. Können Data Trusts unter der DSGVO datenschutzkonform handeln?</b> .....	<b>12</b>
<b>I. Übertragung der Rechtsstellung des Betroffenen</b> .....	<b>12</b>
1. Volle Übertragung des Rechts .....	<b>13</b>
2. Einräumung von Nutzungsrechten .....	<b>13</b>
3. Zusammenfassung .....	<b>14</b>
<b>II. Einräumung von Vertretungsmacht zur Wahrnehmung der Rechte des Betroffenen</b> .....	<b>14</b>
1. Stellvertretung für die Erlaubnis der Verarbeitung .....	<b>14</b>
2. Stellvertretung für die Betroffenenrechte und für die Abwehrbefugnisse .....	<b>16</b>
3. Zwischenergebnis und Zusammenfassung .....	<b>18</b>
<b>III. Datenschutzrechtliche Zulässigkeit ohne Rechtsübertragung</b> .....	<b>18</b>
1. Erlaubnistatbestand .....	<b>18</b>
2. Wahrnehmung der Betroffenenrechte und Geltendmachung von Abwehransprüchen .....	<b>23</b>
3. Weitere Anforderungen und Grundsätze der DSGVO .....	<b>23</b>
<b>D. Mögliche gesetzgeberische oder behördliche Maßnahmen, um die Situation zu verbessern</b> .....	<b>25</b>
<b>I. Regelung einer möglichen Rechtsübertragung in der DSGVO</b> .....	<b>25</b>
<b>II. Regelung der Stellvertretung in der DSGVO</b> .....	<b>25</b>
1. Auf europäischer Ebene .....	<b>25</b>
2. Auf Ebene der Mitgliedstaaten? .....	<b>25</b>
<b>III. Klarstellungen durch Behörden</b> .....	<b>26</b>
<b>E. Ergebnis</b> .....	<b>27</b>
<b>I. Was ist ein Data Trust</b> .....	<b>27</b>
<b>II. Können Data Trusts unter der DSGVO datenschutzkonform handeln?</b> .....	<b>27</b>
<b>III. Wie kann die Lage von Data Trusts verbessert werden?</b> .....	<b>29</b>

## A. Executive Summary

Ausgangsfrage des Gutachtens ist, ob und falls ja, in welcher Form sog. „Data Trusts“ mit dem geltenden Datenschutzrecht, insbesondere der DSGVO, vereinbar sind und – soweit dies nicht der Fall ist – welche Änderungen im Datenschutzrecht erforderlich wären, um Data Trusts zu ermöglichen.

Die kurze Antwort ist: zum Teil. Die lange Antwort, so zeigt sich, ist etwas komplizierter.

### **Was ist ein Data Trust:**

Bei einem Data Trust verwaltet eine natürliche oder juristische Person (der „Data Trust“), für jemand anderen (den „Datengeber“) Daten bzw. Rechte in Bezug auf diese Daten und stellt sie Dritten (den „Datennutzern“) zu deren Zwecken oder auch zu Zwecken der Allgemeinheit zur Verfügung.

Der Data Trust muss in der Lage sein, Datenverarbeitungen der Datennutzer, an die er die Daten weitergeben möchte, zu gestatten. Zudem muss er die Rechte der Datengeber, die ihm ihre Daten anvertraut haben, verteidigen und deren Betroffenenrechte ausüben können. Ein wichtiges Element des Data Trusts ist es auch, dass er ohne die kontinuierliche Mitwirkung der Datengeber agieren kann. Der Data Trust soll eine Treuepflicht gegenüber dem Datengeber haben. Diese entsteht beim Trust automatisch. Bei anderen Formen muss sie durch einen Vertrag geschaffen werden, was im deutschen Recht jedoch ohne Probleme möglich ist.

### **Datenschutzrechtlich stellen sich zur Verwirklichung dieser Ziele drei Fragen:**

1. Erstens, könnte eine Rechtsübertragung vom Datengeber auf den Data Trust stattfinden, so dass der Data Trust aus eigenem Recht diese Funktionen erfüllen kann?
2. Zweitens, könnte der Data Trust in Stellvertretung des Datengebers tätig werden. Er würde dann eigenständig und auf eigene Entscheidung hin aber in fremdem Namen tätig sein?
3. Beide Instrumente sind bis auf eine kleine Ausnahme nicht in der DSGVO geregelt. Es stellt sich also, drittens, die Frage: Können diese Funktionen auch mit den „Bordmitteln“ der DSGVO erfüllt werden?

### **Die rechtliche Prüfung auf Vereinbarkeit mit dem Datenschutzrecht hat folgende Ergebnisse gebracht:**

1. Eine Übertragung des Rechts, Verarbeitungen zu gestatten, Betroffenenrechte oder andere Abwehrrechte wahrzunehmen, ist unter der DSGVO nicht möglich.
2. Eine Stellvertretung ist in Bezug auf die Geltendmachung von Abwehrrechten bei rechtswidriger Datenverarbeitung nach Art. 80 Abs. 1 DSGVO für gewisse Organisationen zulässig.
3. Eine Stellvertretung im Übrigen ist in der DSGVO nicht ausdrücklich vorgesehen, und es ist unstritten, ob sie möglich ist. Es lässt sich rechtlich vertretbar eine Stellvertretungsmöglichkeit be-

gründen. Es besteht aber aufgrund einer strittigen Rechtslage und mangels einer eindeutigen Positionierung von Gerichten und/oder Datenschutzbehörden ein rechtliches Risiko, dass ein solches Vorgehen – ebenso rechtlich vertretbar – von Gerichten und/oder Behörden als rechtswidrig eingestuft wird.

4. Zudem muss im Falle der Stellvertretung beachtet werden, dass ein Data Trust nach dem deutschen Rechtsdienstleistungsgesetz möglicherweise erlaubnispflichtige Rechtsdienstleistungen erbringt. Dies gilt insbesondere für die Geltendmachung von Betroffenenrechten und für die Geltendmachung von Abwehrbefugnissen. In diesem Fall wäre, ohne eine ausdrückliche gesetzliche Gestattung der Tätigkeit, der Betrieb eines Data Trusts auch aus dieser Perspektive mit Rechtsunsicherheiten verbunden.
5. Die Erlaubnis zur Übermittlung der Daten der Datengeber an Datennutzer lässt sich rechtlich vertretbar auch unter dem geltenden Recht konstruieren, insbesondere über einen Vertrag zwischen Data Trust und Datennutzer (Art. 6 Abs. 1 lit. b) DSGVO), aber auch über das berechtigte Interesse (Art. 6 Abs. 1 lit. f) DSGVO) sowie eine Einwilligung (Art. 6 Abs. 1 lit. a) DSGVO) jeweils ggf. in Verbindung mit einer Zweckänderung nach Art. 6 Abs. 4 DSGVO. Eine Verarbeitung besonderer Kategorien personenbezogener Daten ist – jedenfalls in den meisten Fällen – nur mit Einwilligung möglich (Art. 9 DSGVO).

Sämtliche dieser Lösungen sind allerdings mit Rechtsunsicherheiten verbunden, so dass auch hier ein rechtliches Risiko dabei besteht, die Datenverarbeitungen auf diese Erlaubnistatbestände zu stützen.

6. Bei der Wahrnehmung der Betroffenenrechte und bei der Geltendmachung von Abwehrbefugnissen kommt man allerdings um eine Stellvertretung nicht herum. Hierfür gelten die geschilderten Erkenntnisse.

### **Die Lage von Data Trusts kann auf mehreren Wegen verbessert werden:**

1. Der Optimalfall wäre es, wenn der europäische Gesetzgeber neben Verantwortlichem und Auftragsverarbeiter eine neue Rolle in der DSGVO vorsieht. Diese neue Rolle könnte die Rechte der betroffenen Person innehaben und wahrnehmen.
2. Eine weitere Option wäre es, in der DSGVO ausdrücklich die Möglichkeit einer Stellvertretung zu thematisieren bzw. auszubauen. Sie müsste sowohl auf Ebene der Erlaubnistatbestände, also Art. 6 DSGVO, als auch auf Ebene der Betroffenenrechte, Art. 12 ff. DSGVO und der gerichtlichen Geltendmachung, Art. 77 - 79 DSGVO, ermöglicht werden.
3. Schließlich würde es unter dem geltenden Recht helfen, wenn die Aufsichtsbehörden Rechtsunsicherheiten beseitigen würden. So könnte der Europäische Datenschutzausschuss Stellung zu dem Themenkomplex der Stellvertretung unter der DSGVO nehmen oder zu der Frage, ob Verarbeitungen über Art. 6 Abs. 1 lit. b) DSGVO gerechtfertigt werden können, die selbst Leistungsgegenstand des Vertrags sind.

## B. Was ist ein Data Trust?

Am Anfang des Gutachtens steht die Frage, was ein Data Trust eigentlich ist. Der Data Trust als Begriff und als Rechtsform ist noch nicht fest etabliert, sondern im Wandel.<sup>1</sup> Der Begriff lehnt sich an die Rechtsfigur des Trusts an, eine dogmatische Konstruktion des englischen Rechts, die im deutschen Rechtskreis nicht ohne weiteres geläufig und gebräuchlich ist.

Es soll daher zunächst (*I. Was ist ein Trust und welche Rechtsbeziehungen bestehen in ihm?*) kurz beleuchtet werden, was ein „Trust“ ist und welche Merkmale er hat. Anschließend wird darauf aufbauend untersucht, was ein „Data Trust“ ist, welche Grundmerkmale er hat und welche verschiedenen rechtlichen Formen derzeit diskutiert werden (*II. Was ist ein Data Trust?*), um einen Data Trust zu verwirklichen. Schließlich kann dann beurteilt werden, welche Merkmale und inwieweit für die datenschutzrechtliche Beurteilung relevant sind (*III. Datenschutzrechtliche Problem-  
punkte*).

### I. Was ist ein Trust und welche Rechtsbeziehungen bestehen in ihm?

Trusts können eine Vielzahl unterschiedlicher Formen und Variationen annehmen. Hinzu kommt, dass es nicht das „eine“ Trust-Recht gibt, sondern sich insbesondere die rechtlichen Auswirkungen eines Trusts von Rechtsordnung zu Rechtsordnung unterschei-

den. Um das Gutachten in einem überschaubaren Rahmen zu halten, können daher nur die grundlegenden Eigenschaften eines Trusts betrachtet werden. Ausgegangen wird dabei vom Trust, wie er sich im englischen Recht entwickelt hat.

#### 1. Grundaufbau des Trusts

Der Trust stammt rechtsgeschichtlich aus dem englischen Rechtskreis und stellt eine Form der unselbständigen Stiftung dar.<sup>2</sup> Rechtlich unselbständig bedeutet hier, dass der Trust als Sondervermögen selbst keine juristische Person, also kein eigenes Rechtssubjekt ist.<sup>3</sup> Rechtssubjekte sind ausschließlich die beteiligten (juristischen oder natürlichen) Personen: der „Settlor“, der ein Vermögen, eine Sache oder ein Recht (das „Trust-Vermögen“) einer weiteren Person, dem „Trustee“ zuwendet. Das Trust-Vermögen vermischt sich nicht mit dem Vermögen des Trustee, sondern bleibt zu jeder Zeit selbständig. Der Trustee wiederum darf das Trust-Vermögen nur zugunsten eines Dritten, des „beneficiary“ verwenden. Dritter können hierbei bestimmte einzelne Personen oder Personengesamtheiten („private trust“), aber – unter gewissen Bedingungen – auch ein öffentlicher oder gemeinnütziger Zweck sein („charitable trust“ oder „public trust“). Die Grundlagen, insbesondere die Zweckbindung, der der Trustee unterworfen ist, werden in der jeweiligen Errichtungsurkunde des Trusts festgelegt.<sup>4</sup> Die Gründung des Trusts selbst kann dabei sowohl als Rechts-

1 Blankertz, *Designing Data Trusts: Why We Need to Test Consumer Data Trusts Now*, 2020, S. 24, 26, abrufbar unter: [https://www.stiftung-nv.de/sites/default/files/designing\\_data\\_Trusts\\_e.pdf](https://www.stiftung-nv.de/sites/default/files/designing_data_Trusts_e.pdf); s. auch Hardinges, *Data Trusts in 2020*, abrufbar unter: <https://theodi.org/article/data-trusts-in-2020/>.

2 Jakob, in: *Münchener Handbuch des Gesellschaftsrechts*, Band 5, 4. Aufl. 2016, § 119 Rn. 56.

3 Jakob, in: *Münchener Handbuch des Gesellschaftsrechts*, Band 5, 4. Aufl. 2016, § 119 Rn. 54.

4 Jakob, in: *Münchener Handbuch des Gesellschaftsrechts*, Band 5, 4. Aufl. 2016, § 119 Rn. 57.

geschäft, als auch auf einer gesetzlichen Grundlage geschehen.<sup>5</sup>

Die beschriebene Dreieckskonstellation ist üblich, aber nicht zwingend. Eine Person kann im Rahmen des Trusts auch mehrere der beschriebenen Rollen einnehmen. So kann beispielsweise der Settlor auch personenidentisch mit dem Trustee oder dem Beneficiary sein.<sup>6</sup>

Diese Grundlagen des Trusts spiegeln sich auch in dem Haager Trustübereinkommen<sup>7</sup> („HTÜ“) wider, welches die internationale Anerkennung von Trusts regelt und in Art. 2 HTÜ definiert:

„Ein Trust hat folgende Eigenschaften:

- a) das Vermögen des Trusts stellt ein getrenntes Sondervermögen dar und ist nicht Bestandteil des persönlichen Vermögens des Trustees;
- b) die Rechte in Bezug auf das Vermögen des Trusts lauten auf den Namen des Trustees oder auf den einer anderen Person in Vertretung des Trustees;
- c) der Trustee hat die Befugnis und die Verpflichtung, über die er Rechenschaft abzulegen hat, das Vermögen in Übereinstimmung mit den Trustbestimmungen und den ihm durch das Recht auferlegten besonderen Verpflichtungen zu verwalten, zu verwenden oder darüber zu verfügen.“

## 2. Rechtliche Konsequenzen der Einrichtung eines Trusts

Die Einrichtung eines Trusts hat rechtliche Konsequenzen für den Settlor, den Trustee und den Beneficiary.

### a) Vollständiger Rechtsverlust des Settlor und vollständiger Rechtserwerb des Trustee

Die erste, und rechtlich am leichtesten zu erfassende, Konsequenz ist der vollständige Rechtsübergang vom Settlor auf den Trustee. Soweit sich der Settlor nicht selbst als Trustee oder Beneficiary einsetzt, behält er keine Rechte zurück. Der Settlor hat grundsätzlich auch keine Ansprüche mehr gegenüber dem Trustee, wenn dieser sich nicht an den dem Trust zugrundeliegenden Zweck hält; insbesondere besteht keine vertragsrechtlich fortwirkende Verpflichtung des Trustee gegenüber dem Settlor. Der Settlor hat nur die Möglichkeit, sich vorzubehalten, den Trustee unter bestimmten Voraussetzungen abzusetzen oder auszutauschen.<sup>8</sup> Es handelt sich damit im Wesentlichen um eine gewöhnliche Rechtsübertragung, wie sie auch im deutschen Recht bekannt ist.

### b) Zusätzlicher Rechtserwerb beim Beneficiary

Die tatsächliche Besonderheit des Trusts ergibt sich vielmehr aus der Rechtsstellung des Beneficiaries und dessen Rechten gegenüber dem Trustee. Der Beneficiary erhält eine eigene Rechtsstellung, die ihm insbesondere das Recht gibt, bei einem Missbrauch des Trust-Vermögens („breach of trust“) gegen den Trustee vorzugehen. Es handelt sich hierbei nicht um einen vertraglichen Anspruch des Beneficiaries. Der Beneficiary erhält insbesondere auch kein Eigentum am Trust-Vermögen, auch wenn bei der Beschreibung der Rechtsstellung zur Vereinfachung teilweise von

<sup>5</sup> von Bar, EuZW 2018, 925.

<sup>6</sup> von Bar, EuZW 2018, 925.

<sup>7</sup> 30. Convention on the law applicable to Trusts and on their recognition (concluded 1 July 1985), abrufbar unter: <https://assets.hcch.net/upload/conventions/txt30en.pdf>.

<sup>8</sup> von Bar, EuZW 2018, 925, 926.

„gespaltenem“ Eigentum zwischen Beneficiary und Trustee gesprochen wird.

Die Einzelheiten und Klassifizierungen sind äußerst umstritten. Geläufig ist die Bezeichnung als eine besondere Erscheinungsform eines beschränkten dinglichen Rechts oder als ein zwischen Schuld- und Sachenrechten schwankendes Recht eigener Art.<sup>9</sup> Ein eher für eine schuldrechtliche Verpflichtung (sprich: nur zwischen Trustee und Beneficiary wirkend) sprechendes Merkmal der Rechtsstellung des Beneficiarys ist es, dass er sich – jedenfalls im Grundsatz<sup>10</sup> – gegen Beeinträchtigung durch Dritte nicht wehren kann. Seinem Recht fehlt also die im deutschen Recht für dingliche Rechte wesentliche Abwehrfunktion. Diese Befugnisse stehen nur dem Trustee zu.<sup>11</sup>

Sachenrechtsähnliche (sprich: eine Wirkung gegenüber gegenüber entfaltend) Eigenschaft des Rechts des Beneficiarys ist dagegen, dass es insolvenzfest ist und insbesondere, dass es bei einer trustwidrigen Veräußerung nicht zu einem Rechtsverlust, sondern zu einer Surrogation kommt, also sich die Rechte des Beneficiarys an der im Austausch gegen das trustwidrig veräußerte Vermögen erlangten Sache, Gegenstand oder Recht fortsetzen.<sup>12</sup>

### 3. Zusammenfassung

Zusammenfassend ist der Trust also ein selbst nicht rechtsfähiges Sondervermögen, dem eine Dreiecks-konstellation zwischen Settlor, Trustee und Beneficiary zugrundeliegt. Der Settlor überträgt auf Grundlage einer Errichtungsurkunde seine vollständige Rechtsposition an den Trustee, der alleiniger Inhaber des Rechts wird. Der Beneficiary erhält dabei ebenfalls ein originäres Recht, mit dem er im Falle eines

trustwidrigen Handelns gegen den Trustee vorgehen kann. Dieses Recht hat teilweise schuldrechtliche (keine Abwehrfunktion) und teilweise sachenrechtliche Komponenten (Insolvenzfestigkeit, Surrogation bei Veräußerung).

## II. Was ist ein Data Trust?

Es stellt sich als nächstes die Frage, was nun darauf aufbauend ein *Data Trust* ist und auf welche unterschiedliche Art und Weise er rechtlich konstruiert werden kann.

### 1. Die Grundidee des Data Trusts

Beim Data Trust wird die Grundidee des Trusts – jemand verfügt über ein Recht, Vermögen oder einen Gegenstand zugunsten und im Interesse einer anderen Person – in den digitalen Bereich übertragen. Die Bezugspunkte des Data Trusts sind dabei Daten, oder genauer gesagt, die Rechte an den Daten. Die Daten sollen entweder im Interesse desjenigen, der sie an den Trust gegeben hat, oder aber zugunsten öffentlicher Zwecke geschützt und Dritten zur Verfügung gestellt werden, damit sie die Daten nutzen können. Der Data Trust soll dabei möglichst eigenständig und ohne Mitwirkung des ursprünglichen Datengebers handeln können.<sup>13</sup>

Weshalb dies erforderlich ist, wird unterschiedlich begründet. Es lassen sich jedoch vereinfacht vier Argumente zusammenfassen. Zum einen, um ein Machtungleichgewicht zwischen den Individuen und den Datenverarbeitenden auszugleichen, da den Individuen – gerade im Zuge komplexer technischer Verfahren – schlicht das Know-how und die Zeit fehle, um

9 von Bar, EuZW 2018, 925, 926 mit weiteren Nachweisen.

10 Eine wesentliche Ausnahme ist, wenn der Trustee selbst bei Rechtsverletzungen nicht tätig wird. Weitere Ausnahmen beschrieben bei von Bar, EuZW 2018, 925, 926 f.

11 von Bar, EuZW 2018, 925, 926 f.

12 von Bar, EuZW 2018, 925, 927 f.

13 S. im Überblick: *Hardinges*, Data Trusts in 2020, abrufbar unter: <https://theodi.org/article/data-Trusts-in-2020/>; Anouk Ruhaak, Data Trusts: Why, What and How, abrufbar unter: <https://algorithmwatch.org/en/data-Trusts-why-what-and-how/>; *Blankertz*, Designing Data Trusts: Why We Need to Test Consumer Data Trusts Now, 2020, S. 24, 26, abrufbar unter: [https://www.stiftung-nv.de/sites/default/files/designing\\_data\\_Trusts\\_e.pdf](https://www.stiftung-nv.de/sites/default/files/designing_data_Trusts_e.pdf); *Delacroix/Lawrence*, Bottom-up data Trusts: disturbing the 'one size fits all' approach to data governance, International Data Privacy Law, Volume 9, Issue 4, November 2019, S. 236, 240, 245 f.



ihre durch das Datenschutzrecht gewährten Rechte geltend machen zu können.<sup>14</sup> Zweitens gebe es Datenmonopole bei einzelnen großen Unternehmen, deren Nutzung für den Einzelnen nur schwer umgangen werden könne, wodurch die Freiwilligkeit der Entscheidung des Einzelnen untergraben werde.<sup>15</sup> Ein drittes Argument ist, dass den gesellschaftlichen Interessen an der Verarbeitung von personenbezogenen Daten nicht genüge getan werde und insbesondere das Teilen von Daten, das zu gesellschaftlichem Fortschritt führen könne, erschwert werde, gerade auch mit Hinblick auf die Entwicklung von Künstlicher Intelligenz und Machine-Learning.<sup>16</sup> Schließlich wird das Datenmonopol großer Unternehmen auch kritisch gesehen, da so kleineren Unternehmen der Markteintritt und damit letztlich Wettbewerb erschwert werde.<sup>17</sup>

## 2. Verschiedene rechtliche Formen zur Konstruktion eines Data Trusts

Ob der Data Trust dabei auch ein Trust im rechtlichen Sinn sein muss oder soll, wird unterschiedlich beurteilt, und es werden neben der rechtlichen Ausgestaltung als Trust auch andere rechtliche Formen in Betracht gezogen. Es sind dabei die nachfolgend beschriebenen Varianten im Gespräch, welche die Ziele

des Data Trust mit unterschiedlichen juristischen Mitteln umsetzen.<sup>18</sup>

— **Data Trust als Trust:** Ein sehr verbreiteter Vorschlag ist der, den den Data Trust als Trust im eigentlichen Sinne auszugestalten.<sup>19</sup> Hierbei wäre derjenige, der die Rechte an den Daten dem Trust einräumt, der Settlor und gleichzeitig auch der Beneficiary. Der Data Trust würde die Rolle des Trustee übernehmen. Der Vorteil wird darin gesehen, dass in einem Trust automatisch die treuhänderischen Pflichten entstehen und die jeweiligen Rechtsübergänge und Rechtsstellungen zwischen den Beteiligten vorgegeben sind. Was in der Diskussion häufig zu kurz kommt, ist die Beschäftigung mit der Frage, wie der Betroffene seine Rechtsmacht zur Gestattung von Verarbeitungen an den Data Trust übertragen soll (also Art. 6 Abs. 1 DSGVO). Stattdessen wird sich eher auf die Betroffenenrechte (also Art. 12 ff. DSGVO) konzentriert.<sup>20</sup> Zudem wird – wobei hier nicht ganz auszuschließen ist, dass dies auf einem anderen Rechtsverständnis gründet – nur davon gesprochen, dass diese Rechte „mandatable“, also im Deutschen *in Stellvertretung* wahrgenommen werden können. Ob dies möglich ist, ist auch ein Problem, aber ein anderes Problem. Nach den obigen Befunden nimmt ein Trust

14 *Delacroix/Lawrence*, Bottom-up data Trusts: disturbing the ‘one size fits all’ approach to data governance, International Data Privacy Law, Volume 9, Issue 4, November 2019, S. 236, 239; Jesus College Cambridge, Note of a workshop sponsored by The Alan Turing Institute and Jesus College Intellectual Forum, abrufbar unter: [http://files-eu.clickdimensions.com/turingacuk-ap7zg/files/datatrusts-23sept-at9jan.pdf?1579608631917&\\_cldee=amFJay5oYXJkaW5nZXNAdGh2R2Rm9yZWw%3D%3D&recipientid=contact-bfce7509a09ce811814270106faae7f1-c45479e0841549f7ab1a5df63f6d4f77&esid=fb5a5344-463c-ea11-a812-002248076b40](http://files-eu.clickdimensions.com/turingacuk-ap7zg/files/datatrusts-23sept-at9jan.pdf?1579608631917&_cldee=amFJay5oYXJkaW5nZXNAdGh2R2Rm9yZWw%3D%3D&recipientid=contact-bfce7509a09ce811814270106faae7f1-c45479e0841549f7ab1a5df63f6d4f77&esid=fb5a5344-463c-ea11-a812-002248076b40).

15 *Ruhaak*, Data Trusts: Why, What and How, abrufbar unter: <https://algorithmwatch.org/en/data-trusts-why-what-and-how/>.

16 *Reed*, BPE solicitors and Pinsent Masons, Data Trusts: legal and governance considerations (2019), S. 10; *Hardinges*, Data Trusts in 2020, abrufbar unter: <https://theodi.org/article/data-trusts-in-2020/>; Open Data Institute, Data Trusts: lessons from three pilots, 2019, abrufbar unter: <https://theodi.org/article/odi-data-trusts-report/>.

17 *Blankertz*, Designing Data Trusts: Why We Need to Test Consumer Data Trusts Now, 2020, S. 11, abrufbar unter: [https://www.stiftung-nv.de/sites/default/files/designing\\_data\\_trusts\\_e.pdf](https://www.stiftung-nv.de/sites/default/files/designing_data_trusts_e.pdf), die jedoch auf S. 7 genauso die oben genannten Punkte des ersten Lagers aufnimmt; beide Punkte ebenfalls aufgreifend: *Bundesministerium für Wirtschaft und Energie*, Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft, Bericht der Kommission Wettbewerbsrecht 4.0, 2019, S. 43 f.; abrufbar unter: [https://www.bmwi.de/Redaktion/DE/Publikationen/Wirtschaft/bericht-der-kommission-wettbewerbsrecht-4-0.pdf?\\_\\_blob=publicationFile&v=10;%20;Datenethikkommission](https://www.bmwi.de/Redaktion/DE/Publikationen/Wirtschaft/bericht-der-kommission-wettbewerbsrecht-4-0.pdf?__blob=publicationFile&v=10;%20;Datenethikkommission), Gutachten der Datenethikkommission, S. 133 ff., abrufbar unter: [https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?\\_\\_blob=publicationFile&v=5](https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=5); in die Richtung von Platform Governance argumentiert: *McDonald*, The Fiduciary Supply Chain, 2019, abrufbar unter: <https://www.cigionline.org/articles/fiduciary-supply-chain>.

18 *S.* zum Überblick: *Reed/bpe Solicitors/Pinsent Masons*, Data trusts: legal and governance considerations, 2019, S. 14 ff., abrufbar unter: <https://theodi.org/wp-content/uploads/2019/04/General-legal-report-on-data-trust.pdf>.

19 *Delacroix/Lawrence*, Bottom-up data Trusts: disturbing the ‘one size fits all’ approach to data governance, International Data Privacy Law, Volume 9, Issue 4, November 2019, S. 236, 239; *Lau/Penner/Wong*, The Basics of private und public data trusts, NUS Law Working Paper 2019/019, 2019, abrufbar unter: <http://law.nus.edu.sg/wps/>.

20 *Delacroix/Lawrence*, Bottom-up data Trusts: disturbing the ‘one size fits all’ approach to data governance, International Data Privacy Law, Volume 9, Issue 4, November 2019, S. 236 245.

nämlich gerade nicht die Rechte stellvertretend wahr, sondern wird selbst zum Rechtsinhaber. Dies stellt gerade eines der wesentlichen Merkmale eines Trusts dar.

- **Der Data Trust als Gesellschaft:** In dieser Konstellation ist der Data Trust eine eigene rechtsfähige Person, der die Datengeber Rechte an den Daten einräumen, und die wiederum die Befugnis zur Nutzung der Daten an die Datennutzer einräumt. Dabei werden sowohl „klassische“ Gesellschaften (in Deutschland beispielsweise eine GmbH) als auch gemeinnützige Formen der Gesellschaften (im englischen Recht beispielsweise die CIC, im deutschen Recht wäre es bspw. ein gemeinnütziger Verein oder eine gemeinnützige GmbH) als potenzielle Typen angesehen.<sup>21</sup> Die treuhänderische Bindung, die dem Trust immanent ist, müsste hier auf vertraglichem Wege zwischen Datengeber und Data Trust vereinbart werden. Dies stößt jedenfalls im deutschen Recht auf keine Probleme, da allgemein anerkannt ist, dass treuhänderische Pflichten auf vertraglichem Wege vereinbart werden können.<sup>22</sup> Die Fähigkeit, mit den Daten unabhängig agieren zu können, wäre konstruktiv hier über eine Rechtsübertragung wie beim Trust denkbar. Daneben könnte man in dieser Konstellation aber auch eine Stellvertretungsform wählen, die dem Data Trust die rechtsgeschäftliche Vollmacht zum Abschluss der Verträge mit den Datennutzern einräumt. Damit würde es keiner weiteren Mitwirkung des Datengebers bedürfen.

Eine Sonderform des Data Trusts als Gesellschaft ist der Data Trust als gesetzlich geschaffene Organisation.<sup>23</sup> In diesem Fall wäre zunächst ein Tätigwerden des Gesetzgebers erforderlich, der ein konkretes Regelwerk aufstellt.

- **Data Trust als Vertragsnetzwerk:** Ein weiterer Vorschlag ist es, ein Vertragsnetzwerk zu schaffen, bei dem der Datengeber mit dem Data Trust sowie mit den Datennutzern jeweils Verträge schließt und damit ein verzweigtes Vertragsnetz zwischen allen Parteien entsteht, bei dem jeder gegenüber jedem vertragliche Verpflichtungen eingeht.<sup>24</sup> Über diese Grundzüge hinaus sind im Einzelnen hier noch viele Fragen offen. Insbesondere wurde im Rahmen des Vorschlags noch nicht spezifiziert, inwieweit der Datengeber selbst in die Vertragsschlüsse involviert sein muss. Dies würde dem Sinn und Zweck des Data Trusts, dass er möglichst eigenständig agieren kann, zuwiderlaufen. Diesem Hemmnis könnte man dadurch begegnen, dass man auch hier – wie beim Data Trust als Gesellschaft beschrieben – dem Data Trust gestattet, mit rechtsgeschäftlicher Vollmacht im Namen des Betroffenen zu handeln.

### III. Datenschutzrechtliche Problempunkte

Nicht alle Merkmale des Data Trusts werfen datenschutzrechtliche Probleme auf. So ist das Datenschutzrecht etwa indifferent gegenüber der gesellschaftsrechtlichen Ausgestaltung, also zum Beispiel, welche Gesellschaftsform ein Trust einnehmen muss. Auch die (sei es vertraglich, gesetzlich oder durch Trust begründete) Pflicht des Data Trusts, nur im Interesse des Datengebers oder eines öffentlichen Zwecks zu handeln, ist datenschutzrechtlich zunächst nicht von Belang.

Datenschutzrechtlich relevant ist dagegen die Befugnis des Data Trusts, über die Weitergabe der personenbezogenen Daten zu bestimmen und Betroffenenrechte sowie Abwehrbefugnisse (also zum

21 *Reed/bpe Solicitors/Pinsent Masons*, Data trusts: legal and governance considerations, 2019, S. 17 f., abrufbar unter: <https://theodi.org/wp-content/uploads/2019/04/General-legal-report-on-data-trust.pdf>.

22 S. zur Treuhand im BGB *Schubert*, in: Münchener Kommentar zum BGB, 8. Aufl. 2018, § 164 BGB Rn 51 ff. und insb. auch *Schäfer*, in: Münchener Kommentar zum BGB, 8. Aufl. 2020, § 662 BGB Rn. 31 ff.

23 *Reed/bpe Solicitors/Pinsent Masons*, Data trusts: legal and governance considerations, 2019, S. 16, abrufbar unter: <https://theodi.org/wp-content/uploads/2019/04/General-legal-report-on-data-trust.pdf>.

24 *Reed/bpe Solicitors/Pinsent Masons*, Data trusts: legal and governance considerations, 2019, S. 14., abrufbar unter: <https://theodi.org/wp-content/uploads/2019/04/General-legal-report-on-data-trust.pdf>.

Beispiel Unterlassungsansprüche oder Schadensersatzansprüche) gegenüber dem Datennutzer oder Dritten geltend machen zu können.

Ganz abstrakt betrachtet, kann dieses Ziel auf zwei Wegen erreicht werden: Entweder der Data Trust (bzw. in der Terminologie des Trusts der Trustee) wird selbst der Rechtsinhaber, oder der Data Trust nimmt die Rechte des Datengebers, also des Betroffenen, als dessen Stellvertreter und mit dessen Vertretungsmacht wahr. Im nächsten Abschnitt muss daher geklärt werden, ob diese beiden Modelle mit dem geltenden Datenschutzrecht vereinbar sind. Schließlich stellt sich auch, soweit dies nicht oder nicht vollständig der Fall ist, die Frage, ob ein Data Trust auch ohne die Möglichkeiten einer Rechtsübertragung oder eines Handelns in Stellvertretung rechtmäßig handeln könnte.

## C. Können Data Trusts unter der DSGVO datenschutzkonform handeln?

Die zentrale Frage des Gutachtens ist, ob und ggf. wie Data Trusts in Übereinstimmung mit der DSGVO verwirklicht werden können.

Wir haben im vorherigen Schritt gelernt, dass ein Data Trust vor allem zwei datenschutzrechtlich relevante Dinge können muss: Er muss, erstens, über die Weitergabe der personenbezogenen Daten bestimmen, also selbständig eine Datenverarbeitung der Daten der Datengeber gestatten können, und, zweitens, die Betroffenenrechte sowie weitere Abwehrbefugnisse (also zum Beispiel Unterlassungsansprüche oder Schadensersatzansprüche) gegenüber den Datennutzern oder Dritten geltend machen können.

Klassischerweise lassen sich solche Ziele im Recht entweder dadurch erreichen, dass man das Recht selbst überträgt, oder vom Rechtsinhaber zu dessen Wahrnehmung bevollmächtigt wird, also in Stellvertretung für den Rechtsinhaber handelt. Daher wird im Folgenden zunächst untersucht, ob es im geltenden Recht möglich ist, diese Rechte entweder voll oder jedenfalls teilweise auf den Data Trust zu übertragen, oder ob sie in Stellvertretung wahrgenommen werden können.

Abschließend wird untersucht, ob die Ziele des Data Trusts möglicherweise im geltenden Datenschutzrecht auch ohne diese beiden Rechtsinstitute verwirklicht werden können.

### I. Übertragung der Rechtsstellung des Betroffenen

Es soll zunächst untersucht werden, ob der Datengeber dazu in der Lage ist, seine Rechte auf den Data Trust zu übertragen. Dies wäre insbesondere erforderlich, um einen Trust im eigentlichen Sinne zu erstellen.<sup>25</sup> Eine Rechtsübertragung als Grundlage wäre aber auch im Gesellschafts-Modell möglich.

Zunächst kann hier ohne weiteres festgestellt werden, dass dem Datengeber als der gem. Art. 4 Nr. 1 DSGVO betroffenen Person, aus der DSGVO die Rechte zustehen, Datenverarbeitungen zu gestatten und auch Betroffenenrechte oder andere Abwehrrechte, wie Schadensersatzansprüche u.ä., geltend zu machen. Eine Gestattung der Datenverarbeitungen kann die betroffene Person zum Beispiel jederzeit mittels einer Einwilligung nach Art. 6 Abs. 1 lit. a) DSGVO vornehmen. Die Betroffenenrechte und der Schadensersatzanspruch sind in den Art. 15 ff. DSGVO und 82 DSGVO geregelt.

Fraglich ist alleine, ob der Datengeber diese Rechte und Rechtsstellungen auch übertragen kann. Eine Übertragung kann entweder insgesamt (sog. translativ Rechtsübertragung), oder nur in Teilen (sog. konstitutiv Rechtsübertragung) geschehen. Die konstitutiv Rechtsübertragung wäre in etwa vergleichbar mit der Einräumung von Nutzungsrechten (umgangssprachlich „Lizenzen“) im Urheberrecht.<sup>26</sup>

25 Dies verkennen anscheinend *Delacroix/Lawrence*, Bottom-up data Trusts: disturbing the 'one size fits all' approach to data governance, *International Data Privacy Law*, Volume 9, Issue 4, November 2019, S. 236, 240, 245 f., die stets nur von „mandatable rights“, also von Stellvertretung sprechen und sich zudem auch nicht auf die Erlaubnis der Verarbeitung sondern nur die Betroffenenrechte beziehen.

26 Zu den Rechtsübertragungen im Urheberrecht: *Ohly*, in: Schricker/Loewenheim, Urheberrecht, § 31 UrhG Rn. 9 ff.; *Wandtke/Grunert*, in: Wandtke/Bullinger, Urheberrecht, 5. Aufl. 2019, Vorbemerkung vor §§ 31 ff. Rn. 21 ff.; zur Übertragbarkeit des Rechts auf informationelle Selbstbestimmung aus der Perspektive des Grundgesetzes und des deutschen Zivilrechts: *Funke*, Dogmatik und Voraussetzungen der datenschutzrechtlichen Einwilligung im Zivilrecht, 2017, Kapitel 2 § 3, S. 38 ff. je mwNachw.

Weder die volle Rechtsübertragung, noch die Einräumung von ausschnittsweisen Nutzungsrechten sind in der DSGVO ausdrücklich vorgesehen, was freilich nicht zwingend bedeuten muss, dass sie auch verboten sind. Es wird sich aber sogleich zeigen, dass die besseren Gründe dafür sprechen, dass eine Übertragung der Rechte nicht möglich ist.

## 1. Volle Übertragung des Rechts

Die DSGVO dient dem Schutz der Grundrechte und Grundfreiheiten der betroffenen Personen (Art. 1 Abs. 2 DSGVO). Konsequenterweise knüpfen daher die Befugnisse, die Datenverarbeitung per Einwilligung zu gestatten oder Betroffenenrechte sowie Schadensersatz geltend zu machen, direkt im Wortlaut der Art. 6 Abs. 1 lit. a) DSGVO und Art. 15 ff. DSGVO an die Betroffeneneneigenschaft an. Die jeweiligen Befugnisse stehen nur der betroffenen Person zu. Eine volle Übertragung der Rechte und Befugnisse würde in der Systematik der DSGVO letztlich nichts anderes bedeuten, als dass der Data Trust selbst zur betroffenen Person würde und die damit verbundenen Befugnisse damit auf ihn übergingen.

Es sprechen letztlich sehr viele Gründe dagegen, dass eine solche Möglichkeit besteht. Erstens sieht die DSGVO eine feste Definition der betroffenen Person in Art. 4 Nr. 1 DSGVO vor, nämlich die identifizierbare oder identifizierte natürliche Person, auf die sich die in den personenbezogenen Daten enthaltenen Informationen beziehen (Art. 4 Nr. 1 DSGVO). Eine Übertragung der Betroffenenstellung ist unter dieser Definition nicht möglich. Zweitens sprechen aber auch jenseits des eigentlichen Normtextes Sinn und Zweck der DSGVO gegen diese Möglichkeit. Die DSGVO sieht zum Schutze der betroffenen Person eine Vielzahl an Rechten und Pflichten vor, die zudem grundrechtlich

über Art. 8 GRCh<sup>27</sup> garantiert sind. Eine Rechtsübertragung würde bedeuten, dass sich die betroffene Person jeglichen Schutzes ihrer personenbezogenen Daten entledigt, also in diesem Bereich einen vollständigen Grundrechtsverzicht ausübt. Ein Grundrechtsverzicht ist in der Rechtsprechung des EuGH und des EGMR zwar hinsichtlich bestimmter Grundrechte anerkannt,<sup>28</sup> die DSGVO steuert jedoch mit ihrem ausdifferenzierten Normensystem den Grundrechtsverzicht gewissermaßen in gelenkte Bahnen, um ihn in Abwägung mit den Interessen der Allgemeinheit auszugestalten. Eine pauschale Übertragung würde dieses austarierte System, das der Gesetzgeber bewusst vorgegeben hat, letztlich umgehen.<sup>29</sup>

## 2. Einräumung von Nutzungsrechten

Neben der Vollübertragung der Betroffenenstellung stößt aber auch die teilweise Übertragung der Rechtsstellung in Form von Nutzungsrechten auf Bedenken.

Hinsichtlich der Entscheidung über die Gestattung der Datenverarbeitung hat die DSGVO ausdrückliche und abschließende Regelungen in Art. 6 DSGVO getroffen. Dabei hat sie dem Betroffenen neben der Möglichkeit, Verträge zu schließen (Art. 6 Abs. 1 lit. b) DSGVO) und damit mittelbar die damit verbundenen Verarbeitungen zu rechtfertigen, genau ein Instrument an die Hand gegeben, welches es ihm gestattet, Datenverarbeitungen zu genehmigen: die Einwilligung nach Art. 6 Abs. 1 lit. a) DSGVO. Art. 6 Abs. 1 lit. a) DSGVO setzt vom Wortlaut aber wiederum an den Betroffenen an. Nur der Betroffene, und sonst niemand, darf mittels einer Einwilligung die Verarbeitung gestatten. Zudem muss man sich vor Augen führen, was eine Rechtsübertragung hier im Ergebnis bedeuten würde: Die betroffene Person hätte keine Möglichkeit mehr, über die Verarbeitung zu bestimm-

27 CHARTA DER GRUNDRECHTE DER EUROPÄISCHEN UNION (2010/C 83/02), ABl. EU vom 30. März 2010, C 83, S. 389 (im Folgenden: GRCh).

28 *EuGH*, C-41/79 – Testa, Slg.1980, 1979 Rn.18 f.; *EGMR*, Nr.1620/03 v. 23.9.2010 Rn.71; *Jarass*, in: *Jarass*, GRCh, 3. Aufl. 2016, Art. 52 GRCh Rn. 18.

29 Oder in etwas „blumigeren“ Worten des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit: „*Personenbezogene Daten sind aber kein beliebiges Handelsobjekt, sondern stets Teil einer bestimmten natürlichen Person, deren Menschenwürde unveräußerlich ist. Unter anderem aus dieser Menschenwürde leitet sich auch das Recht auf informationelle Selbstbestimmung ab. Beim handlungsbezogenen Ansatz würden diese Teile der Person dem Schutz der Würde entzogen und zum reinen Handelsobjekt herabgestuft. Der Gedanke vom Menschen als Rohstoff ist mit unserer gesellschaftlichen Ordnung jedoch nicht vereinbar.*“, Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Tätigkeitsbericht 2017 – 2018, S. 35.

men. Auch dies kann nach den Erwägungen zur Vollrechtsübertragung nicht vom europäischen Verordnungsgeber bezweckt gewesen sein.

Entsprechende Bedenken bestehen in Bezug auf die Betroffenenrechte und sonstige Abwehrrechte, die die DSGVO gewährt. Sie knüpfen, wie die Einwilligung, ausdrücklich im Gesetz an die Betroffenenstellung an. Eine Übertragung ist daher nicht denkbar.

### 3. Zusammenfassung

Zusammenfassend lässt sich damit festhalten, dass eine Übertragung der Rechtsstellung des Betroffenen, sei es vollständig oder auch nur teilweise, unter dem geltenden Recht nicht möglich ist. Ein Data Trust kann damit – jedenfalls von datenschutzrechtlicher Seite her und unter dem geltenden Recht – nicht in der Form eines Trusts erstellt werden. Auch einem Data Trust in Form einer Gesellschaft können nicht die Rechte der Datengeber übertragen werden.

## II. Einräumung von Vertretungsmacht zur Wahrnehmung der Rechte des Betroffenen

Allerdings könnte eine Ausübung der Befugnisse in Stellvertretung möglich sein, so dass zumindest eine Ausgestaltung des Data Trusts in Form eines Gesellschafts- oder Vertragsmodells in Frage kommen könnte. Der Data Trust wäre in dieser Konstellation, da er – anders als bei der Rechtsübertragung – nicht in die Rechtsstellung der betroffenen Person einrückt, gleichwohl aber über Zwecke und Mittel der Datenverarbeitung bestimmen würde, ein eigener Verantwortlicher nach Art. 4 Nr. 7 DSGVO.

Grundvoraussetzung der Stellvertretungskonstellation ist es, dass der Datengeber mit dem Data Trust einen Vertrag schließt und ihn damit beauftragt, seine Interessen wahrzunehmen und Daten weiterzugeben bzw. seine Betroffenen- oder Abwehrrechte wahrzunehmen und im Rahmen dieses Vertrags dem Data Trust Vertretungsmacht nach § 164 BGB einräumt.

Systematisch müssen auch hier wieder die Erlaubnis zur Datenverarbeitung (Art. 6 DSGVO), insbesondere für die Datenweitergabe an die Datennutzer, von der Geltendmachung der Betroffenen- und Abwehrrechte (Art. 12 ff. DSGVO) unterschieden werden.

### 1. Stellvertretung für die Erlaubnis der Verarbeitung

Möglicherweise kann der Data Trust im Rahmen der Erlaubnis der Weitergabe (Art. 6 Abs. 1 DSGVO) als Stellvertreter des Datengebers auftreten und damit ohne dessen Mitwirkung im Einzelfall eine Erlaubnis zur Weitergabe geschaffen werden. Als konkrete Erlaubnistatbestände kommen hier zwei in Betracht, nämlich, erstens, eine Einwilligung, abgegeben durch den Data Trust im Namen des Datengebers (Art. 6 Abs. 1 lit. a) DSGVO), oder, zweitens, ein Vertrag, den der Data Trust im Namen des Datengebers mit dem Datennutzer schließt, und der über Art. 6 Abs. 1 lit. b) DSGVO die Verarbeitung rechtfertigen könnte.

#### a) In Stellvertretung abgegebene Einwilligung

Es stellt sich als Erstes die Frage, ob eine Einwilligung in Stellvertretung abgegeben werden kann.

Dies ist in der deutschen Literatur äußerst umstritten und wird teilweise bejaht,<sup>30</sup> teilweise aber auch verneint.<sup>31</sup> Die Befürworter stellen im Wesentlichen auf die Freiheit des Betroffenen ab, selbst entscheiden

30 *Ingold*, in: Sydow, Europäische Datenschutzgrundverordnung, Art. 7 DSGVO Rn. 19; *Specht*, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 9 Rn. 42; *Buchner/Kühling*, in: Kühling/Buchner, DSGVO BDSG 2. Aufl. 2018, Art. 7 DSGVO Rn. 31.

31 *Ernst*, ZD 2017, 110 (111); *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 DSGVO Rn. 37; *Taeger*, in: Taeger/Gabel, DSGVO, 3. Aufl. 2019, Art. 7 DSGVO Rn. 10; *Schulz*, in: Gola, DSGVO, 2. Aufl. 2018, Art. 7 DSGVO Rn. 9.

zu können, wer für ihn welche Erklärungen abgibt.<sup>32</sup> Zudem sei die Stellvertretung ein europarechtlich anerkanntes Institut.<sup>33</sup> Dagegen wird aber eingewendet, dass die DSGVO selbst eine Stellvertretung nicht vorsieht.<sup>34</sup> In der Tat spricht der Wortlaut von Art. 6 Abs. 1 lit. a) DSGVO dafür, dass keine Stellvertretung möglich ist, da dort eben nur der Betroffene erwähnt wird. Auch findet sich, anders als beispielsweise in Art. 8 Abs. 3 DSGVO keine ausdrückliche Öffnungsklausel zugunsten des mitgliedstaatlichen Vertragsrechts, welches Einfallstor für eine Stellvertretung sein könnte. Schließlich lässt sich auch ein weiteres Argument, die Stellvertretung sei Ausdruck der Entscheidungsfreiheit des Betroffenen<sup>35</sup>, in die andere Richtung wenden, indem man betont, dass mit einer Stellvertretung bei der Einwilligung vor allem die Schutzmechanismen des Datenschutzrechts ausgehebelt werden.

Ebenfalls gegen die Möglichkeit einer Stellvertretung könnten Art. 8 Abs. 1 DSGVO und Art. 80 Abs. 1 DSGVO sprechen. Art. 8 Abs. 1 DSGVO regelt die Stellvertretung in einem Sonderfall bei Kindern, Art. 80 Abs. 1 DSGVO sieht eine Regelung vor, die Stellvertretung bei der gerichtlichen Geltendmachung von Ansprüchen für privilegierte Organisationen ermöglicht. Hieraus könnte man den Umkehrschluss ziehen, dass die DSGVO in den übrigen Fällen eine Stellvertretung nicht ermöglicht und insbesondere auch die Mitgliedstaaten keine Befugnis haben, eine Stellvertretung zu regeln. Dies ist aber nicht zwingend, da man genauso gut argumentieren könnte, dass die DSGVO die Möglichkeit der Stellvertretung allgemein anerkennt und zugrunde legt und hier nur besonders für die gerichtliche und behördliche Geltendmachung hervorhebt.

Es gibt damit kein eindeutiges Ergebnis. Aus der Systematik der DSGVO und ihres Charakters als geschlossenem Regelwerk, in dem in Bezug auf die Einwilligung eine Stellvertretung eben nicht ausdrücklich

normiert ist, überwiegen leicht die Argumente gegen die Möglichkeit, eine Stellvertretung, insbesondere aus dem mitgliedstaatlichen Recht, zuzulassen.

Das bedeutet also im Ergebnis, dass es rechtlich zwar vertretbar ist, die Stellvertretung bei der Einwilligung zuzulassen. Es besteht aber ein rechtliches Risiko, dass eine Aufsichtsbehörde oder ein Gericht in diesem Fall ebenso rechtlich vertretbar zu dem gegenteiligen Ergebnis kommt. Die Stellvertretungskonstellation bietet hier also eine vertretbare, nicht aber rechtssichere Lösung.

### **b) Stellvertretung im Rahmen von Art. 6 Abs. 1 lit. b) DSGVO**

Eine weitere Möglichkeit wäre es, sich das von der DSGVO nicht direkt erfasste Vertragsrecht zu Nutze zu machen. In diesem Fall würde der Data Trust stellvertretend im Namen des Datengebers Verträge mit den Datennutzern abschließen, welche die Datenverarbeitung zum Leistungsgegenstand haben. Für den Vertragsschluss selbst, welcher nicht der DSGVO, sondern dem jeweiligen nationalen Zivilrecht unterliegt, ist eine Stellvertretung unproblematisch nach § 164 BGB möglich.

Man könnte dann überlegen, ob die entsprechende Verarbeitung in Folge des Vertrags, der in Stellvertretung zwischen Datennutzer und Datengeber zustande gekommen ist, mittels Art. 6 Abs. 1 lit. b) DSGVO gerechtfertigt werden kann. Art. 6 Abs. 1 lit. b) DSGVO verlangt, dass die Verarbeitung für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, erforderlich sein muss.

Im in Stellvertretung geschlossenen Vertrag zwischen Betroffenen und Datennutzer wäre die Gestattung der Datenverarbeitung letztendlich die Hauptleistungspflicht. In der datenschutzrechtlichen Literatur

32 *Ingold*, in: Sydow, Europäische Datenschutzgrundverordnung, Art. 7 DSGVO Rn. 19; *Buchner/Kühling*, in: Kühling/Buchner, DSGVO BDSG, 2. Aufl. 2018, Art. 7 DSGVO Rn. 31; *Specht*, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 9 Rn. 42.

33 *Ingold*, in: Sydow, Europäische Datenschutzgrundverordnung, Art. 7 DSGVO Rn. 19.

34 *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmman, Datenschutzrecht, 2019, Art. 7 DSGVO Rn. 37; daher lehnt wohl auch *Delacroix/Lawrence*, Bottom-up data Trusts: disturbing the 'one size fits all' approach to data governance, International Data Privacy Law, Volume 9, Issue 4, November 2019, S. 236, 246 die Möglichkeit einer Stellvertretung unter dem geltenden Recht ab.

35 *Specht*, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 9 Rn. 42.

werden gegen derartige Konstruktionen aber Bedenken vorgebracht. Art. 6 Abs. 1 lit. b) DSGVO solle hiernach nur solche Verarbeitungen erfassen, bei denen die Datenverarbeitung akzessorisch zu den Vertragsleistungen ist. Sie soll aber eben gerade nicht Vertragsgegenstand selbst sein, da es sonst an der Erforderlichkeit mangle und die gesetzlichen Voraussetzungen der Einwilligung zu Lasten der betroffenen Person umgangen würden.<sup>36</sup> Auch der Europäische Datenschutzausschuss<sup>37</sup> hat Bedenken dagegen, personenbezogene Daten als Vertragsgegenstand zuzulassen, und bevorzugt in diesen Konstellationen eine Einwilligung als Rechtsgrundlage. Letztere Ansicht des Datenschutzausschusses dürfte aber in Anbetracht von Artikel 3 der Richtlinie über digitale Inhalte<sup>38</sup> in Zukunft zumindest sehr zweifelhaft sein, da dort Transaktionen wie „Leistung gegen Daten“ ausdrücklich anerkannt werden.

Aber auch im Übrigen spricht Vieles gegen diese Ansicht, insbesondere, dass sich diese Einschränkung nicht aus der DSGVO ergibt und sie auch nicht vom Sinn und Zweck gerechtfertigt ist. Zwar ist es korrekt, dass die Einwilligung besondere Anforderungen zum Schutz des Betroffenen an die Erklärung stellt.<sup>39</sup> Doch müssen auch beim Vertrag die wesentlichen Vertragsbestandteile („essentialia negotii“) zwischen den Parteien übereinstimmend erklärt werden, was letztendlich auch nichts anderes bedeutet, als dass der Betroffene eine informierte Erklärung abgibt. Zudem bietet das Zivilrecht über AGB-Kontrollen und Billigkeitsinstrumente wie Treu und Glauben (§ 242 BGB) hinreichende Schutzmaßnahmen für die betroffene Person. Rechtlich ist es daher gut vertretbar, das Stellvertretungsmodell in dieser Form zu gestalten.

Insgesamt sprechen hier also die überzeugenderen und auch belastbaren Argumente dafür, dass sich auch solche Verarbeitungen über Art. 6 Abs. 1 lit. b) DSGVO rechtfertigen lassen.

Gleichwohl ist die Gegenansicht immer noch rechtlich vertretbar. Es bleibt daher, insbesondere aufgrund der ablehnenden Haltung des Europäischen Datenschutzausschusses, auch hier ein rechtliches Risiko bestehen, dass eine Behörde oder ein Gericht dieser dargestellten Gegenauffassung folgt und es grundsätzlich nicht gestattet, die Verarbeitung auf Art. 6 Abs. 1 lit. b) DSGVO zu stützen.

Daher gilt auch hier, dass eine Stellvertretungskonstruktion rechtlich möglich, aber nicht rechtssicher ist.

## 2. Stellvertretung für die Betroffenenrechte und für die Abwehrbefugnisse

Gegen die Stellvertretung bei der Geltendmachung von Betroffenenrechten und der Geltendmachung von Abwehrbefugnissen gelten mehrere der oben gemachten Einwände nicht. Insbesondere wird in keiner Weise der Schutz des Betroffenen übergangen.

Art. 80 Abs. 1 DSGVO regelt dementsprechend für die gerichtliche Geltendmachung von Abwehrbefugnissen bei rechtswidrigen Datenverarbeitungen nach Art. 79 DSGVO, dass diese auch von bestimmten privilegierten Organisationen<sup>40</sup> in Stellvertretung wahrgenommen werden dürfen. Das bedeutet, dass, wenn ein Data Trust die Anforderungen von Art. 80 Abs. 1 DSGVO erfüllt, er bereits unter dem geltenden Recht in Stellvertretung für die betroffene Person handeln darf. Fällt er dagegen nicht unter die nach Art. 80

36 *Schantz*, in: Simitis/Hornung/Spiecker gen. Döhmman, Datenschutzrecht, 2019, Art. 6 DSGVO Rn. 33.

37 *Europäischer Datenschutzausschuss*, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, S. 15 Rn. 54, abrufbar unter: [https://edpb.europa.eu/our-work-tools/public-consultations/2019/guidelines-22019-processing-personal-data-under-article-61b\\_de](https://edpb.europa.eu/our-work-tools/public-consultations/2019/guidelines-22019-processing-personal-data-under-article-61b_de).

38 RICHTLINIE (EU) 2019/770 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 20. Mai 2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen, ABl. EU, L 136 v. 22. Mai 2019.

39 Darum verneinend: *Schantz*, in: Simitis/Hornung/Spiecker gen. Döhmman, Datenschutzrecht, 2019, Art. 6 DSGVO Rn. 33.

40 Konkret: eine Einrichtung, Organisation oder Vereinigung ohne Gewinnerzielungsabsicht, die ordnungsgemäß nach dem Recht eines Mitgliedstaats gegründet ist, deren satzungsmäßige Ziele im öffentlichem Interesse liegen und die im Bereich des Schutzes der Rechte und Freiheiten von betroffenen Personen in Bezug auf den Schutz ihrer personenbezogenen Daten tätig ist.



Abs. 1 DSGVO privilegierten Organisationen, darf er im Umkehrschluss nicht in Stellvertretung für diese Abwehrbefugnisse tätig werden.

### a) **Datenschutzrechtliche Bedenken bei der Stellvertretung für Betroffenenrechte**

Die Stellvertretung im Falle von Betroffenenrechten ist dagegen nicht ausdrücklich geregelt. Es bestehen auch hier Bedenken. Eine Stellvertretung ist – jedenfalls im deutschen Recht – nämlich dann nicht möglich, wenn ein Anspruch höchstpersönlicher Natur ist.<sup>41</sup> Dass dies bei Art. 15 DSGVO der Fall ist, hat das Oberverwaltungsgericht Lüneburg entschieden.<sup>42</sup> Es begründet dabei seine Entscheidung im Wesentlichen mit Literatur zur Rechtslage vor dem Inkrafttreten der DSGVO und mit der Wichtigkeit des Anspruchs für die Rechte des Betroffenen.<sup>43</sup>

Dieses Ergebnis kann rechtlich aber nicht vollends überzeugen, da es den datenschutzrechtlichen Auskunftsanspruch damit in eine Riege mit anderen höchstpersönlichen Rechten, wie der Eheschließung, der Vaterschaftsanfechtung, Testamentserrichtung u.ä. stellt, was von der Wertung der jeweils mit diesen Geschäften verbundenen Rechtsfolgen nicht angemessen erscheint.<sup>44</sup> Gleichwohl lässt sich aber auch hier anführen, dass die Ansprüche eben ausdrücklich nur dem Betroffenen zustehen und eine Stellvertretung in der DSGVO nicht weiter geregelt ist und damit aufgrund ihres abschließenden Charakters auch nicht bestehen darf. Es bestehen damit – auch wenn man nicht die deutsche Figur der höchstpersönlichen Ansprüche bemühen möchte – jedenfalls rechtliche Bedenken gegen eine Geltendmachung von Betroffenenrechten in Stellvertretung, so dass hier ein gewisses rechtliches Risiko erhalten bleibt.

### b) **Exkurs: Bedenken aufgrund des Rechtsdienstleistungsgesetzes**

Es soll noch ein weiterer – nicht datenschutzrechtlicher – Problembereich erwähnt werden, da dieser in Bezug auf die Betroffenenrechte und sonstige Abwehrrechte ein erhebliches Hindernis sein dürfte. Das deutsche Recht enthält mit dem Rechtsdienstleistungsgesetz<sup>45</sup> (RDG) eine sehr strenge Beschränkung des Marktes für Rechtsdienstleistungen. Eine Rechtsdienstleistung ist dabei nach § 2 Abs. 1 RDG jede Tätigkeit in konkreten fremden Angelegenheiten, sobald sie eine rechtliche Prüfung des Einzelfalls erfordert.

Rechtsdienstleistungen dürfen nur erbracht werden, wenn sie ausdrücklich gesetzlich erlaubt sind. Rechtsdienstleistungen erbringen dürfen ansonsten in aller Regel nur zugelassene Rechtsanwälte oder in sehr beschränktem Umfang Personen mit Inkassolizenz. Nach § 5 Abs. 1 RDG dürfen Rechtsdienstleistungen zudem erbracht werden, wenn sie als Nebenleistung zum Berufsbild gehören, was aber eher restriktiv ausgelegt wird.

Zwar wird man Art. 80 Abs. 1 DSGVO in dessen Anwendungsbereich als eine solche gesetzliche Erlaubnis ansehen können. Im Übrigen besteht aber die Gefahr, dass eine Prüfung der Rechtslage im Einzelfall, zum Beispiel der Anspruchsvoraussetzungen, erforderlich ist und damit auch ein Data Trust unter § 2 Abs. 1 RDG fallen könnte. Es bliebe dann nur die Möglichkeit, einen Rechtsanwalt oder eine Rechtsanwaltskanzlei entsprechend für diese Prüfungen zu involvieren. Der konkrete Data Trust sollte hier jedoch sehr genau prüfen, was inwieweit erforderlich ist.

41 S. nur: *Schubert*, in: Münchener Kommentar zum BGB, 8. Aufl. 2018, § 164 BGB, Rn. 100.

42 *OVG Lüneburg*, Urteil vom 20.6.2019 – 11 LC 121/17, ZD 2019, 473.

43 *OVG Lüneburg*, Urteil vom 20.6.2019 – 11 LC 121/17, ZD 2019, 473, 475 Rn. 49 ff.

44 Ähnlich insoweit auch aus Perspektive des englischen Rechts: *Delacroix/Lawrence*, Bottom-up data Trusts: disturbing the 'one size fits all' approach to data governance, *International Data Privacy Law*, Volume 9, Issue 4, November 2019, S. 236, 246.

45 Rechtsdienstleistungsgesetz vom 12. Dezember 2007 (BGBl. I S. 2840), das zuletzt durch Artikel 8 des Gesetzes vom 20. November 2019 (BGBl. I S. 1724) geändert worden ist.

### 3. Zwischenergebnis und Zusammenfassung

Es lässt sich damit zusammenfassen:

Eine Rechtsübertragung ist im Datenschutzrecht nicht möglich. Ein Data Trust als Trust im eigentlichen Sinne kann daher unter der geltenden Rechtslage nicht geschaffen werden.

Der Data Trust könnte jedoch die Form einer Gesellschaft annehmen, der Stellvertretungsmacht eingeräumt wird, oder eines Vertragsnetzwerks. Der Datengeber kann hier nach rechtlich vertretbarer Ansicht sowohl eine Stellvertretung zur Erteilung einer Einwilligung, als auch – rechtlich noch etwas besser vertretbar – zum Abschluss von Verträgen mit dem Datennutzer konstruieren. Ebenfalls rechtlich möglich ist die Geltendmachung von Betroffenenansprüchen und Abwehrrechten.

Gleichwohl bestehen für alle Lösungen rechtliche Risiken. Es handelt sich überwiegend um nicht ausdrücklich in der DSGVO adressierte Thematiken, und in sämtlichen entscheidungserheblichen Fragen existieren rechtlich vertretbare Gegenmeinungen, die insbesondere auch von Behörden und Gerichten vertreten werden. Dabei sollte auch in Betracht gezogen werden, dass es sich hier gerade um die zentralen Elemente des Data Trusts handelt, von dem die Rechtmäßigkeit des gesamten übrigen Handelns abhängt. Diese auf eine unsichere Rechtslage zu gründen, birgt ein erhebliches Risiko.

### III. Datenschutzrechtliche Zulässigkeit ohne Rechtsübertragung

Es bleibt damit letztlich zu klären, ob sich auch ohne Rückgriff auf die oben beschriebenen Instrumente der Rechtsübertragung oder Einräumung einer Stellvertretung die Ziele eines Data Trusts verwirklichen lassen. Hierfür benötigt der Data Trust insbesondere einen Erlaubnistatbestand zur Weitergabe der Daten an die Datennutzer und eine Berechtigung zur Wahrnehmung der Betroffenenrechte, und er muss die

übrigen Anforderungen der DSGVO erfüllen, die nur kurz gestreift werden sollen.

#### 1. Erlaubnistatbestand

Der Data Trust benötigt eine Erlaubnis zur Weitergabe der Daten an den jeweiligen Datennutzer nach Art. 6 DSGVO. Art. 6 DSGVO stellt mehrere Erlaubnistatbestände zur Verfügung. Hier kommen insbesondere die Einwilligung, Art. 6 Abs. 1 lit. a) DSGVO, die Verarbeitung zur Erfüllung eines Vertrags, Art. 6 Abs. 1 lit. b) DSGVO, die Verarbeitung für die Erfüllung einer Aufgabe im öffentlichen Interesse, Art. 6 Abs. 1 lit. e) DSGVO, sowie die Verarbeitung zur Wahrung eines berechtigten Interesses, Art. 6 Abs. 1 lit. f) DSGVO, in Frage. Schließlich kommt auch eine Zweckänderung nach Art. 6 Abs. 4 DSGVO und als Sonderkonstellation die Beauftragung des Data Trusts als Auftragsverarbeiter in Frage.

##### a) Einwilligung nach Art. 6 Abs. 1 lit. a) DSGVO

Der Datengeber könnte dem Data Trust eine Einwilligung zur Weitergabe erteilen. Die Einwilligung ist grundsätzlich in allen Verarbeitungssituationen geeignet, eine Datenverarbeitung zu rechtfertigen. Soweit besondere Kategorien von personenbezogenen Daten (Art. 9 DSGVO) verarbeitet werden, ist sie in der Regel sogar das einzige dafür geeignete Instrument.

Die Einwilligung ist nach Art. 4 Nr. 11 DSGVO definiert als jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Die Einwilligung muss also freiwillig, in informierter Weise, unmissverständlich und für den bestimmten Fall abgegeben werden.

Während die Kategorien der Freiwilligkeit, Informiertheit und Unmissverständlichkeit im Falle eines Data Trusts grundsätzlich keine Probleme bereiten dürf-

ten, sieht dies bei der Abgabe für den bestimmten Fall anders aus, da hier der Kreis der erfassten Datenverarbeitungen, einschließlich der Zwecke und Datenempfänger, vorhersehbar sein muss.<sup>46</sup> Es wäre daher regelmäßig erforderlich, für eine rechtssichere Weitergabe an einen neuen Empfänger und zu einem neuen Zweck, eine neue Einwilligung einzuholen. Man könnte auch für die weiteren Verarbeitungen auf Art. 6 Abs. 1 lit. f) DSGVO oder Art. 6 Abs. 4 DSGVO zurückzugreifen, was aufgrund ihrer offenen Ausgestaltung aber mit Unsicherheiten verbunden ist.<sup>47</sup>

Eine Ausnahme von der ansonsten strengen Auslegung der Bestimmtheit besteht derzeit nur im Bereich der wissenschaftlichen Forschung nach Erwägungsgrund 33 DSGVO. Hiernach soll auch eine Einwilligung in „bestimmte Bereiche wissenschaftlicher Forschung“ möglich sein. Man kann hier also vom Wortlaut der Verordnung her durchaus argumentieren, dass hiervon ebenfalls die Weitergabe an unterschiedliche Forschungsinstitutionen gedeckt ist, solange sie im selben Bereich der wissenschaftlichen Forschung tätig sind. Eine etablierte Rechtspraxis oder gar Rechtsprechung, wie weit dies zu fassen ist und wo die Grenzen sind, gibt es allerdings noch nicht. Legt man demnach ein großzügiges Verständnis zu Grunde, wäre es denkbar, bei Beitritt des Datengebers zum Data Trust eine Einwilligung einzuholen und auch die Datenweitergaben dann auf diese Einwilligung zu stützen.

Die Einwilligung eignet sich damit also – jedenfalls, wenn man keine regelmäßige Interaktion mit dem Betroffenen will – nur für einen Data Trust, der wissenschaftliche Forschung zum Gegenstand hat.

## **b) Erlaubnis nach Art. 6 Abs. 1 lit. b) DSGVO**

Soweit der Data Trust, wie im Gesellschaftsmodell und im Vertragsnetzmodell vorgesehen, mit dem Datengehenden einen Vertrag abschließt, kommt auch Art. 6 Abs. 1 lit. b) DSGVO außerhalb von Stellvertretungskonstellationen in Betracht. Es können hierbei sowohl Datenverarbeitungen gerechtfertigt werden, die durch den Data Trust vorgenommen werden, als auch durch Dritte, da auch diese nach einhelliger Meinung von Art. 6 Abs. 1 lit. b) DSGVO erfasst werden.<sup>48</sup> Es bestehen hier jedoch die oben im Rahmen der Stellvertretungskonstellation behandelten Rechtsunsicherheiten, ob Verträge, deren Leistungsgegenstand selbst die Verarbeitung der personenbezogenen Daten ist, von Art. 6 Abs. 1 lit. b) DSGVO erfasst werden. Bejaht man dies jedoch, so ist eine Rechtfertigung regelmäßig möglich.

Insbesondere dürfte es hier kein Problem darstellen, dass die konkreten Empfänger und konkreten Verarbeitungszwecke bei den Empfängern noch nicht im Vorhinein bekannt sind, jedenfalls soweit der Vertrag zwischen Datengeber und Data Trust sorgfältig ausgestaltet ist und die inneren Mechanismen, Kriterien und Entscheidungen mit dem Datengehenden transparent vereinbart werden.

Eine Grenze stellen hier lediglich die besonderen Kategorien personenbezogener Daten nach Art. 9 DSGVO dar, welche in aller Regel nur mit einer Einwilligung der betroffenen Person verarbeitet werden dürfen.

## **c) Erlaubnis nach Art. 6 Abs. 1 lit. e) DSGVO**

Auch Art. 6 Abs. 1 lit. e) DSGVO kann auf den ersten Blick eine mögliche Rechtsgrundlage bieten. Allerdings handelt es sich hierbei wie eine Zusammen-

46 *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmman, Datenschutzrecht, 2019, Art. 7 DSGVO Rn. 68; S. auch: *Buchner/Kühling*, in: Kühling/Buchner, DSGVO BDSG, 2. Aufl. 2018, Art. 7 DSGVO Rn. 61.

47 Dazu s. sogl. unter C.III.1.d) Erlaubnis nach Art. 6 Abs. 1 lit. f) DSGVO und S. zur Treuhand im BGB *Schubert*, in: Münchener Kommentar zum BGB, 8. Aufl. 2018, § 164 BGB Rn 51 ff. und insb. auch *Schäfer*, in: Münchener Kommentar zum BGB, 8. Aufl. 2020, § 662 BGB Rn. 31 ff.

48 S. statt aller: *Schulz*, in: Gola, DSGVO, 2. Aufl. 2018, Art. 6 DSGVO Rn. 28; *Albers/Veit*, in: BeckOK DatenschutzR, 33. Ed. 1.5.2020, Art. 6 DSGVO Rn. 30; *Schantz*, in: Simitis/Hornung/Spiecker gen. Döhmman, Datenschutzrecht, 2019, Art. 6 Abs. 1 DSGVO Rn. 22.

schau aus Art. 6 Abs. 2 und Abs. 3 DSGVO lediglich um eine sog. Scharniernorm, die einer weiteren Rechtsgrundlage, nämlich der Festlegung der öffentlichen Aufgabe und der Übertragung auf den jeweils Verantwortlichen, bedarf.<sup>49</sup> Gestattet ist danach eine Verarbeitung, wenn sie für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt. Ohne gesonderte (und noch zu schaffende) gesetzliche Grundlage, welche die Verarbeitung rechtfertigt, kann Art. 6 Abs. 1 lit. e) DSGVO nicht herangezogen werden.

#### **d) Erlaubnis nach Art. 6 Abs. 1 lit. f) DSGVO**

Eine Rechtfertigung der Weitergabe kann auch nach Art. 6 Abs. 1 lit. f) DSGVO möglich sein. Nach Art. 6 Abs. 1 lit. f) DSGVO ist eine Verarbeitung erlaubt, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen.

„Berechtigte Interessen“ wird hierbei weit als jedes wirtschaftlich, rechtlich oder ideell anerkanntswerte Interesse verstanden<sup>50</sup>, und es wird häufig sowohl ein berechtigtes Interesse des Data Trusts an der Verteilung der Daten als auch des Datennutzers in Bezug auf sein konkret verfolgtes Ziel vorliegen, zu dessen Wahrung die Verarbeitung erforderlich ist.

Ein Punkt, der dagegen im jeweiligen Einzelfall geprüft werden muss und problematisch sein kann, ist, ob die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen. Es handelt sich hier um eine umfangreiche Interessenabwägung, in die alle Umstände der konkreten Verarbeitung einbezogen werden müssen. Insbesondere muss hierbei Rücksicht auf die vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zum

Verantwortlichen beruhen (Erwägungsgrund § 47 S.1 DSGVO), genommen werden.<sup>51</sup> Die weiteren zu beachtenden Umstände der Verarbeitung können beispielsweise sein: Interventionsmöglichkeiten, Verkettung der Daten, beteiligte Akteure, Dauer der Verarbeitung, Datenkategorien, Umfang der Datenverarbeitung und der Kreis der betroffenen Personen.<sup>52</sup>

Der Data Trust müsste, wenn er sich auf Art. 6 Abs. 1 lit. f) DSGVO stützen möchte, demnach in jedem Fall eine besonders gute und transparente Information und Darstellung seiner Ziele und seiner Auswahlkriterien anstreben, um so die Erwartungen der betroffenen Personen an die Verarbeitung entsprechend zu formen. Nur wenn der Datengeber wirkliche und vollumfängliche Kenntnis über die geplanten Vorgänge hat, ist eine Rechtfertigung über Art. 6 Abs. 1 lit. f) DSGVO denkbar. Ihm zugutekommen würde die treuhänderische Bindung mit dem Datengeber, die freilich vertraglich festgelegt werden müsste. Hinsichtlich der übrigen Kriterien müsste eine Fall-zu-Fall-Entscheidung vorgenommen werden, wie stark die Rechte der Datengeber durch die Verarbeitung im Data Trust betroffen sind und ob ggf. die des Data Trusts und der Dritten überwiegen. Es liegt hier ein fließender Maßstab vor. Je umfangreicher die Datenverarbeitung, je größer der Kreis der Empfänger und je länger die Daten verarbeitet werden, umso höher ist die Rechtsbeeinträchtigung der betroffenen Personen, und desto eher werden deren Rechte überwiegen.

Eine Möglichkeit, um die Beeinträchtigung der Datengeber gering zu halten, wäre es, Interventions- und Mitbestimmungsmöglichkeiten für sie zu schaffen, damit sie in Einzelfällen bspw. bedingungslos<sup>53</sup> einen Widerspruch gegen die Verarbeitung einlegen könnten. Man könnte sie bspw. vor einer geplanten Übermittlung an einen neuen Empfänger hierüber

49 *Buchner/Petri*, in: Kühling/Buchner, DSGVO BDSG, 2. Aufl. 2018, Art. 6 DSGVO Rn. 114.; *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 6 Abs. 1 DSGVO Rn. 70 f.

50 Statt aller: *Schulz*, in: Gola, DSGVO, 2. Aufl. 2018, Art. 6 DSGVO Rn. 57.

51 S. beispielhaft: *Schantz*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 6 Abs. 1 DSGVO Rn. 105 ff., 108 f.; *Schulz*, in: Gola, DSGVO, 2. Aufl. 2018, Art. 6 DSGVO Rn. 57, 59, 612 je mwNachw.

52 S. hierzu bspw. *Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder*, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, 2019, S. 16 ff., abrufbar unter: [https://www.datenschutzkonferenz-online.de/media/oh/20190405\\_oh\\_tmg.pdf](https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf).

53 Ein Widerspruchsrecht unter besonderen Voraussetzungen besteht nach Art. 21 DSGVO ohnehin.

informieren und ihnen eine gewisse Karenzzeit einräumen, in der sie der Übermittlung widersprechen können. Zudem wäre es für die Abwägung vorteilhaft, mit den Datennutzern genau zu regeln, zu welchen Zwecken und wie lange sie die Daten verwenden dürfen. Je mehr Einfluss der Data Trust behält und je geringer die Gefahr ist, dass die Daten bei den Datennutzern weiterverteilt werden, umso eher lässt sich ausschließen, dass die Interessen des Datengebers überwiegen.

Es lassen sich bei einer sorgfältigen Ausgestaltung Verarbeitungen rechtlich vertretbar auf Art. 6 Abs. 1 lit. f) DSGVO stützen. Es muss allerdings auch berücksichtigt werden, dass gerade in Bezug auf die Weitergabe von personenbezogenen Daten die Behörden traditionell kritisch sind, was die Rechtfertigung aufgrund von Art. 6 Abs. 1 lit. f) DSGVO anbelangt, und im Rahmen der Interessenabwägung strenge Maßstäbe anlegen. Zudem kommt auch die bei der Einwilligung angesprochene Unklarheit in Bezug auf die Weiterverarbeitung von Daten, die zu einem anderen Zweck erhoben wurden, hinzu. Daher muss genauso wie bei den übrigen Erlaubnistatbeständen eine gewisse Rechtsunsicherheit in Kauf genommen werden. Um diese gering zu halten, sollte in jedem Fall eine sorgfältige Dokumentation des Abwägungsvorgangs erfolgen.

### **e) Zweckänderung nach Art. 6 Abs. 4 DSGVO**

Eine weitere Möglichkeit, Verarbeitungen zu legitimieren, ist die sog. Zweckänderung nach Art. 6 Abs. 4 DSGVO. Sie ermöglicht unter gewissen Voraussetzungen die Nutzung von personenbezogenen Daten, die ursprünglich zu einem anderen Zweck erhoben wurden.

#### **(1) Anwendungsbereich Art. 6 Abs. 4 DSGVO**

Fraglich ist, wann Art. 6 Abs. 4 DSGVO für Data Trusts überhaupt zur Anwendung kommen würde. So dürfte für eine Anwendbarkeit bei einer Rechtfertigung

über Art. 6 Abs. 1 lit. b) DSGVO von vornherein kein Raum sein, da hier der Zweck die Leistungspflichten des Vertrags sind, die von vornherein festgelegt sind. Stützt man die Verarbeitung auf ein berechtigtes Interesse, wäre es potenziell denkbar, dass man die Übermittlung an einen neuen Empfänger auf die Zweckänderung stützen könnte. Es wird jedoch hier angenommen, dass ein Rückgriff auf Art. 6 Abs. 4 DSGVO nicht erforderlich ist, wenn eine hypothetische Neuerhebung ohnehin von einem Erlaubnistatbestand nach Art. 6 Abs. 1 DSGVO gedeckt wäre,<sup>54</sup> was angesichts von Erwägungsgrund 50 S. 5 DSGVO auch überzeugend erscheint. Zudem wäre ansonsten die Weiterverwendung bereits erhobener Daten strenger reglementiert als eine Neuerhebung, was nur schwer begründbar ist. Dann könnte man diese Verarbeitungen aber gleich auf Art. 6 Abs. 1 lit. f) DSGVO stützen, ohne den Umweg über Art. 6 Abs. 4 DSGVO wählen zu müssen.

Es bliebe letztlich die Möglichkeit, die Verarbeitung der Daten zunächst auf eine Einwilligung und danach erfolgende Übermittlungen auf Art. 6 Abs. 4 DSGVO zu stützen. Wobei sich auch hier die Frage stellt, ob man die neue Verarbeitung dann nicht gleich auf Art. 6 Abs. 1 lit. f) DSGVO stützen sollte.

#### **(2) Voraussetzungen Art. 6 Abs. 4 DSGVO**

Eine Verarbeitung soll dann möglich sein, wenn sie mit dem ursprünglichen Zweck als vereinbar angesehen wird. Dies wird bspw. durch Art. 5 Abs. 1 lit. b) DSGVO bei im öffentlichen Interesse liegenden Archivzwecken, wissenschaftlicher oder historischer Forschung oder statistischen Zwecken vermutet. Bei allen anderen Zwecken muss eine Einschätzung der Vereinbarkeit der ursprünglichen mit den neuen Zwecken vom Verantwortlichen vorgenommen werden, welche die Kriterien des Art. 6 Abs. 4 lit. a) bis e) DSGVO berücksichtigt:

- a) jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden,

<sup>54</sup> Taeger, in: Taeger/Gabel, DSGVO BDSG, 3. Aufl. 2019, Art. 6 DSGVO Rn. 141; Assion/Nolte/Veil, in: Gierschmann/Schlender/Stentzel/Veil, DSGVO, 2018, Art. 6 DSGVO Rn. 201 ff. mwNachw.

und den Zwecken der beabsichtigten Weiterverarbeitung,

- b) den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen,
- c) die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten gemäß Artikel 9 verarbeitet werden oder ob personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 verarbeitet werden,
- d) die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen,
- e) das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören können.

Es kommt hier also zu einer Wertungsentscheidung, die letztlich ähnlich der Abwägung nach Art. 6 Abs. 1 lit. f) DSGVO ist.<sup>55</sup> Insbesondere spielen auch hier die vernünftigen Erwartungen der betroffenen Person nach Erwägungsgrund 50 eine Rolle, weshalb auf die dortigen Ausführungen verwiesen werden kann und eine zulässige Weiterverarbeitung unter ähnlichen Gesichtspunkten rechtlich begründbar wäre. Zusätzlich würde der Datennutzer Art. 6 Abs. 1 lit. f) DSGVO als gesonderten Erlaubnistatbestand benötigen.

Zusammenfassend lässt sich damit sagen, dass die Weitergabe an die Datennutzer nach Art. 6 Abs. 4 DSGVO unter ähnlichen Gesichtspunkten gerechtfertigt werden kann, wie dies im Rahmen von Art. 6 Abs. 1 lit. f) DSGVO der Fall ist, dies aber mit denselben Rechtsunsicherheiten verbunden ist.

#### **f) „Erlaubnis“ durch Auftragsverarbeitung**

Man könnte in Betracht ziehen, die erforderliche Rechtfertigung einer Verarbeitung dadurch zu „umgehen“, dass man die Datennutzer als temporäre

Auftragsverarbeiter nach Art. 28 DSGVO für den Data Trust engagiert. Die Konsequenz wäre hier, dass der Data Trust rechtlich gesehen keine Daten an einen Dritten übermitteln müsste. Die Verarbeitung würde als eine eigene Verarbeitung des Data Trusts gelten, die mangels der Datenweitergabe einfacher ohne Einwilligung des Datengebers über Art. 6 Abs. 1 lit. f) DSGVO oder Art. 6 Abs. 4 DSGVO gerechtfertigt werden könnte (hier gilt das soeben Gesagte).

Auftragsverarbeiter ist dabei nach Art. 4 Nr. 8 DSGVO eine Person, die personenbezogene Daten im Auftrag eines Verantwortlichen nur für dessen Zwecke und auf dessen Weisung verarbeitet (Art. 28 Abs. 3 lit. a) DSGVO).

Hier liegt aber zugleich das wesentliche Problem dieser Konstellation. Eine Verarbeitung dürfte immer nur für die Zwecke des Data Trusts und nicht für Zwecke der Datennutzer vorgenommen werden. Ein derartiger Data Trust würde sich wahrscheinlich nur für sehr begrenzte Zwecke eignen und in begrenzten Feldern auf Akzeptanz stoßen.

#### **g) Zusammenfassung**

- Damit lässt sich zusammenfassen, dass die Absicht eines Data Trusts, Daten der Datengeber ohne deren weitere Mitwirkung an Datennutzer weiterzugeben kann, in Fällen wissenschaftlicher Forschung auf die Einwilligung nach Art. 6 Abs. 1 lit. a) DSGVO gestützt werden kann, da die DSGVO hier nach Erwägungsgrund 33 eine weiter gefasste Einwilligung gestattet. Es bleibt in diesen Fällen jedoch insoweit Rechtsunsicherheit, als sich noch keine (gerichtlich überprüfte oder von den Behörden akzeptierte) Rechtspraxis herausgebildet hat, wie weit die Einwilligung tatsächlich gefasst sein darf. Der Wortlaut der DSGVO gestattet allerdings eine relativ weite Formulierung. Im Übrigen könnte man eine Einwilligung nur in Kombination mit weiteren Erlaubnistatbeständen, konkret: Art. 6 Abs. 1 lit. f) DSGVO und Art. 6 Abs. 4 DSGVO, verwenden.

<sup>55</sup> Taeger, in: Taeger/Gabel, DSGVO BDSG, 3. Aufl. 2019, Art. 6 DSGVO Rn. 141.

- Daneben ist es rechtlich vertretbar, bei entsprechender Gestaltung des Vertrags zwischen Data Trust und Datengeber, die Datenweitergabe an die Datennutzer auf Art. 6 Abs. 1 lit. b) DSGVO zu stützen. Mit dem Datengeber müssten insbesondere die Prinzipien, nach denen eine Weitergabe und eine Auswahl der Datennutzer erfolgt, klar und transparent vereinbart werden. Allerdings gibt es auch hier rechtliche Unsicherheit dahingehend, dass teilweise vertreten wird, dass eine Verarbeitung nicht durch Art. 6 Abs. 1 lit. b) DSGVO gerechtfertigt werden kann, wenn sie selbst Leistungsgegenstand des Vertrags ist, was es unmöglich machen würde, die Verarbeitungen auf Art. 6 Abs. 1 lit. b) DSGVO zu stützen. Abgesehen von dieser Unsicherheit wäre Art. 6 Abs. 1 lit. b) DSGVO aber die rechtssicherste Wahl unter den zur Verfügung stehenden Möglichkeiten, da es hier weder zu einer wertungsoffenen Abwägung kommt, noch, wenn die erste Hürde genommen ist, es weitere rechtliche Auslegungsunsicherheiten gibt.
- Eine Rechtfertigung aufgrund des berechtigten Interesses nach Art. 6 Abs. 1 lit. f) DSGVO ist ebenfalls im Prinzip denkbar. Es handelt sich hierbei jedoch um eine Abwägungsnorm, welche erfordert, dass jeder konkrete Data Trust eine Abwägung für sich vornehmen muss. Da die Abwägung sehr wertungsabhängig ist, besteht hier stets die Rechtsunsicherheit, dass eine Behörde oder ein Gericht bei denselben angelegten Kriterien ebenso rechtlich vertretbar zu einem anderen Ergebnis kommt und damit die Verarbeitung letztendlich rechtswidrig wird. Zusätzlich müssten, um die Verarbeitung zu rechtfertigen, ein sehr hoher Maßstab an Transparenz erzeugt werden und ggf. auch Mitwirkungs- und Interventionsmöglichkeiten geschaffen werden, was im Ergebnis auf eine der Vertragslösung sehr ähnliche Ausgestaltung zulaufen dürfte.
- Eine Rechtfertigung über Art. 6 Abs. 4 DSGVO ist sowohl in Kombination mit der Einwilligung (Art. 6 Abs. 1 lit. a) DSGVO) als auch in Kombination mit dem berechtigten Interesse (Art. 6

Abs. 1 lit. f) DSGVO) unter dem gleichen Caveat der Rechtsunsicherheit denkbar.

- Schließlich könnte man an eine Auftragsverarbeitungskonstellation denken. Allerdings muss hier angemerkt werden, dass dann die Datennutzer die personenbezogenen Daten nicht zu eigenen Zwecken verarbeiten dürften, was für viele Datennutzer ein Ausschlusskriterium sein dürfte. Eine solche Konstellation wäre daher wahrscheinlich nur in spezifischen Ausnahmefällen sinnvoll.

Es bleibt damit abschließend das einerseits positive, andererseits aber auch unbefriedigende Ergebnis, dass die Weitergabe der Daten vom Data Trust an die Datennutzer grundsätzlich in rechtlich vertretbarer Weise auf alle genannten Erlaubnistatbestände gestützt werden kann, gleichzeitig aber für jeden Erlaubnistatbestand aus unterschiedlichen Gründen auch Rechtsunsicherheit besteht, da Gerichte oder Behörden mit rechtlich vertretbaren Gründen auch zu einer entgegengesetzten Entscheidung kommen könnten, was die gesamten Datenverarbeitungen rechtswidrig werden ließe. Lediglich eine für jede Übermittlung gesondert eingeholte Einwilligung ist rechtlich nicht angreifbar.

## 2. Wahrnehmung der Betroffenenrechte und Geltendmachung von Abwehransprüchen

Eine eigenständige Wahrnehmung der Betroffenenrechte und Abwehrbefugnisse durch den Data Trust ist dagegen, ohne auf das Institut der Stellvertretung zurückzugreifen, nicht denkbar. Hier gilt das oben Gesagte. Die einzige Alternative wäre die Annahme einer Stellung als Bote, die aber jeweils eine Mitwirkung des Betroffenen erfordern würde.

## 3. Weitere Anforderungen und Grundsätze der DSGVO

Natürlich müsste der Data Trust sämtliche weiteren Grundsätze nach Art. 5 DSGVO und sämtliche Compliance-Pflichten einhalten. Compliance-Pflichten

sind hier insbesondere das Führen von Verarbeitungsverzeichnissen (Art. 30 DSGVO), das Erfüllen der Nachweis- und Rechenschaftspflichten (Art. 5 Abs. 2 DSGVO), die Einrichtung angemessener technischer und organisatorischer Maßnahmen (Art. 32 DSGVO), die Beachtung von Meldepflichten bei Data Breaches (Art. 33 und Art. 34 DSGVO), die Vornahme von Datenschutzfolgenabschätzungen (Art. 36 DSGVO). Je nach Einzelfall und Beteiligung des Data Trusts könnten er und der Datennutzer als gemeinsam Verantwortliche nach Art. 26 DSGVO anzusehen sein. Dies würde erfordern, dass sie einen jeweiligen Vertrag nach Art. 26 DSGVO schließen müssten.

Weitere Grundsätze nach Art. 5 Abs. 1 DSGVO, die bei der Verarbeitung beachtet werden müssen, sind Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit. Bezüglich all dieser Pflichten bestehen jedoch keine Besonderheiten in Bezug auf den Data Trust; insbesondere verhindern sie keine der Gestaltungsvarianten.



## D. Mögliche gesetzgeberische oder behördliche Maßnahmen, um die Situation zu verbessern

Es hat sich also gezeigt, dass im geltenden Recht Defizite bestehen, die die Ausgestaltung eines Data Trusts entweder verhindern oder jedenfalls Rechtsunsicherheiten aussetzen. Es könnten daher folgende Maßnahmen ergriffen werden.

### I. Regelung einer möglichen Rechtsübertragung in der DSGVO

Um einen Trust, der mit personenbezogenen Daten umgeht, als solches möglich zu machen, wäre zwingend eine Änderung der DSGVO erforderlich. Es müsste geregelt werden, dass betroffene Personen teilweise oder auch vollständig ihre Rechte an vertrauenswürdige Organisationen wie Data Trusts abgeben könnten.

Dies könnte beispielsweise durch die Schaffung einer neuen Rolle neben Verantwortlichem und Auftragsverarbeiter erreicht werden. Dies würde zugleich ermöglichen, dass mit dieser Rolle besondere Rechte und Pflichten normiert werden, die verhindern, dass der Schutz der personenbezogenen Daten untergraben wird.

### II. Regelung der Stellvertretung in der DSGVO

#### 1. Auf europäischer Ebene

Eine weitere Möglichkeit wäre es, die Stellvertretung in der DSGVO ausdrücklich zu regeln. Dies könnte so

erfolgen, dass Betroffene beliebigen natürlichen oder juristischen Personen Vertretungsmacht einräumen können. Es könnte aber auch vorausgesetzt werden, dass nur privilegierte Organisationen als Stellvertreter tätig werden können.

Art. 80 Abs. 1 DSGVO enthält bereits eine Regelung, welche ermöglicht, bei rechtswidrigen Datenverarbeitungen privilegierten Organisationen die Vertretungsmacht zur Geltendmachung der Rechte gegenüber Behörden und Gerichten einzuräumen. Diese Regelung könnte dahingehend erweitert werden, dass ebenso die ursprüngliche Geltendmachung der Betroffenenrechte erfasst ist sowie insbesondere auch die Befugnis, eine Datenverarbeitung zu gestatten. Systematisch korrekter wäre es allerdings, diese Regelung nicht in Kapitel 8 der DSGVO, sondern in Kapitel 2 und Kapitel 3 aufzunehmen.

#### 2. Auf Ebene der Mitgliedstaaten?

Fraglich ist, ob die Mitgliedstaaten alleine dazu befugt sind, ohne eine Änderung der DSGVO Stellvertretungsmöglichkeiten zu regeln. Die DSGVO hat grundsätzlich einen abschließenden und vollharmonisierenden Charakter. Sie bildet sowohl Unter- als auch Obergrenze des Datenschutzrechts.<sup>56</sup> In Ihrem Anwendungsbereich ist es den nationalen Gesetzgebern daher grundsätzlich verwehrt, Regelungen zu treffen, soweit ihnen nicht ausdrücklich die Befugnis dazu erteilt ist. Dies gilt also sowohl für Regelungen, die den Schutzstandard erhöhen, als auch für Regelungen, die den Schutzstandard senken.

56 Pötters, in: Gola, DSGVO, 2. Aufl. 2018, Art. 1 DSGVO Rn. 24; Spindler/Dalby, in: Spindler/Schuster, RdeM, 4. Aufl. 2019, Art. 1 DSGVO Rn 1, je mwNachw.; s. ferner die Erwägungsgründe 6 – 11 DSGVO.

Soweit eine Stellvertretung bei der Gestattung der Datenverarbeitung erlaubt werden würde, wäre dies faktisch ein neuer Erlaubnistatbestand. Eine solche Regelung ist dementsprechend aufgrund des abschließenden Charakters<sup>57</sup> von Art. 6 DSGVO nicht möglich.

Für die stellvertretende Geltendmachung von Abwehrbefugnissen hat die DSGVO in Art. 80 Abs. 1 DSGVO selbst schon eine Regelung getroffen. Auch hier ist dementsprechend den Mitgliedstaaten eine davon abweichende oder ausweitende Regelung untersagt.

Umstritten ist in Bezug auf die Betroffenenrechte, ob hier die Regelung einer Stellvertretung möglich wäre. Dies wird teilweise damit bejaht, dass dies die Verpflichtungen der Verantwortlichen nicht berühre,<sup>58</sup> was allerdings aufgrund der dargestellten vollharmonisierenden Wirkung nicht vollständig überzeugt, zumal sich auch der Pflichtenkreis des Verantwortlichen erweitert. Er muss die Betroffenenrechte eben nicht nur gegenüber den Betroffenen selbst, sondern auch gegenüber etwaigen Stellvertretern erfüllen. Man könnte dagegen andenken, ob es sich bei einer Regelung zur Stellvertretung möglicherweise um eine Regelung des allgemeinen Zivilrechts oder des Prozessrechts handelt, die nicht dem Anwendungsbereich der DSGVO unterliegt. Aber auch dieses Argument ist, da die DSGVO eben auch die Rechtsdurchsetzung der in ihr enthaltenen Ansprüche zum Thema hat, angreifbar. Eine mitgliedstaatliche Regelung in diesem Bereich liefe damit Gefahr, europarechtswidrig zu sein.

### III. Klarstellungen durch Behörden

Gesetzliche Änderungen, gerade auf europäischer Ebene, aber auch auf nationaler Ebene, sind schwierig und langwierig. Es hat sich gezeigt, dass jedenfalls in Bezug auf die Gestattung der Verarbeitung und auch, jedenfalls im Anwendungsbereich von Art. 80 Abs. 1 DSGVO, in Bezug auf die Abwehrbefugnisse, wenn auch nicht auf die Betroffenenrechte, schon Regelungen bestehen, die elementare Funktionen des Data Trusts abbilden könnten.

Die Umsetzung und Anwendung der Regelungen leidet jedoch unter der allgemeinen Rechtsunsicherheit, die in vielen Bereichen der DSGVO herrscht. In diesen Bereichen würden schon eindeutige und verbindliche Stellungnahmen – beispielsweise durch den europäischen Datenschutzausschuss nach Art. 70 Abs. 1 lit. e) DSGVO – helfen, Rechtsunsicherheiten zu beseitigen.

Für eine Stellungnahme wären vor allem die Themen interessant, inwieweit eine Stellvertretung im Rahmen der DSGVO gestattet ist und inwieweit in Verträgen die Verarbeitung von Daten der Leistungsgegenstand sein kann. Stellungnahmen zur Abwägung nach Art. 6 Abs. 1 lit. f) DSGVO und zur Bewertung nach Art. 6 Abs. 4 DSGVO wären natürlich auch wünschenswert. Allerdings muss man hier beachten, dass diese Abwägungen sehr vom konkreten Sachverhalt abhängen und daher eine abstrakte Stellungnahme nur begrenzt Rechtssicherheit schaffen kann.

57 Mit Ausnahme von Art. 6 Abs. 3 DSGVO, welcher aber hier – da es nicht um Art. Abs. 1 lit. c) oder e) DSGVO geht – nicht anwendbar ist.

58 *Delacroix/Lawrence*, Bottom-up data Trusts: disturbing the 'one size fits all' approach to data governance, *International Data Privacy Law*, Volume 9, Issue 4, November 2019, S. 236, 247.

## E. Ergebnis

Ausgangsfrage des Gutachtens war, ob, und, falls ja, in welcher Form sog. „Data Trusts“ mit dem geltenden Datenschutzrecht, insbesondere der DSGVO, vereinbar sind und – soweit dies nicht der Fall ist – welche Änderungen im Datenschutzrecht erforderlich wären, um Data Trusts zu ermöglichen. Das lässt sich nur teilweise bejahen.

### I. Was ist ein Data Trust

Wir haben zunächst gelernt, was ein Trust und was ein Data Trust ist. Insbesondere haben wir gelernt, dass bei einem Trust ein wesentliches Element ist, dass der Settlor seine Rechtsstellung aufgibt und an den Trustee diese Rechtsstellung voll überträgt. Ein Data Trust, der also in der Form eines Trusts handeln will, müsste in die Rechtsstellung des Settlers, also des Datengebers, vollständig eintreten. Ein Data Trust ist aber nicht zwingend darauf angewiesen, dass tatsächlich eine Vollrechtsübertragung geschieht. Vielmehr ist es für den Data Trust nur wichtig, dass er überhaupt dazu in der Lage ist, zum einen Datenverarbeitungen der Datennutzer, an die er die Daten weitergeben möchte, zu gestatten. Zum anderen ist es wichtig, dass er die Rechte der Datengeber, die ihm ihre Daten anvertraut haben, verteidigen kann. Ein wichtiges Element des Data Trusts ist es gerade, dass er auch ohne die kontinuierliche Mitwirkung der Datengeber agieren kann. Er soll möglichst eigenständig sein. Der Data Trust soll eine Treuepflicht gegenüber dem Datengeber haben. Diese entsteht beim Trust automatisch. Bei anderen Instituten muss sie durch einen Vertrag geschaffen werden, was im deutschen Recht jedoch ohne Probleme möglich ist.

Dementsprechend ist es aus datenschutzrechtlicher Sicht insbesondere wichtig, dass diese Funktionen unter dem geltenden Datenschutzrecht verwirklicht werden können. Rechtstechnisch gesprochen kommen dazu drei rechtliche Vorgänge in Betracht:

- Erstens könnte eine Rechtsübertragung vom Datengeber auf den Data Trust stattfinden, so dass der Data Trust aus eigenem Recht vorgehen kann (so wie es auch beim ursprünglichen Trust angedacht ist).
- Zweitens könnte der Data Trust in Stellvertretung des Datengebers tätig werden. Er würde dann zwar eigenständig und auf eigene Entscheidung hin, aber in fremdem Namen tätig sein.
- Beide Institute sind bis auf eine kleine Ausnahme nicht in der DSGVO geregelt. Es stellt sich also, drittens, die Frage, ob diese Funktionen auch mit den „Bordmitteln“ der DSGVO erfüllt werden können.

### II. Können Data Trusts unter der DSGVO datenschutzkonform handeln?

Die rechtliche Prüfung auf Vereinbarkeit mit dem Datenschutzrecht hat dabei folgende Ergebnisse gebracht:

1. Eine Übertragung des Rechts, Verarbeitungen zu gestatten, Betroffenenrechte oder andere Abwehrrechte wahrzunehmen, ist unter der DSGVO nicht möglich.

2. Eine Stellvertretung ist in Bezug auf die Geltendmachung von Abwehrrechten bei rechtswidriger Datenverarbeitung nach Art. 80 Abs. 1 DSGVO zulässig, soweit die Vertretung durch eine Einrichtung, Organisation oder Vereinigung ohne Gewinnerzielungsabsicht erfolgt, die ordnungsgemäß nach dem Recht eines Mitgliedstaats gegründet ist, deren satzungsmäßige Ziele im öffentlichen Interesse liegen und die im Bereich des Schutzes der Rechte und Freiheiten von betroffenen Personen in Bezug auf den Schutz ihrer personenbezogenen Daten tätig ist.
  3. Eine Stellvertretung im Übrigen ist in der DSGVO nicht ausdrücklich vorgesehen, und es ist umstritten, ob sie möglich ist. Dies gilt sowohl für das Recht, Datenverarbeitungen zu gestatten (also die Einwilligung nach Art. 6 Abs. 1 lit. a) DSGVO), als auch für die Geltendmachung von Betroffenenrechten oder die Geltendmachung von Abwehrrechten durch andere als die nach Art. 80 Abs. 1 DSGVO privilegierten Organisationen. Es ist rechtlich vertretbar, eine Stellvertretung in diesen drei Punkten für zulässig zu erachten. Zusätzlich gibt es auch die rechtlich vertretbare, aber ebenfalls umstrittene, Möglichkeit, die Gestattung zur Übermittlung der Daten an Datennutzer nicht in Form einer Einwilligung vorzunehmen, sondern durch einen in Stellvertretung geschlossenen Vertrag zwischen Data Trust und Datennutzer (Art. 6 Abs. 1 lit. b) DSGVO). Es lässt sich damit rechtlich vertretbar eine Stellvertretungsmöglichkeit begründen. Es besteht aber aufgrund der strittigen Rechtslage und mangels einer eindeutigen Positionierung von Gerichten und/oder Datenschutzbehörden in den umstrittenen Bereichen ein rechtliches Risiko, dass ein solches Vorgehen rechtlich vertretbar von Gerichten und/oder Behörden als rechtswidrig eingestuft wird.
  4. Zudem muss im Falle der Stellvertretung beachtet werden, dass ein Data Trust nach dem deutschen Rechtsdienstleistungsgesetz möglicherweise erlaubnispflichtige Rechtsdienstleistungen erbringt. Dies gilt insbesondere für die Geltendmachung von Betroffenenrechten und für die Geltendmachung von Abwehrbefugnissen. In diesem Fall wäre ohne eine ausdrückliche gesetzliche Gestattung der Tätigkeit der Betrieb eines Data Trusts auch aus dieser Perspektive mit Rechtsunsicherheiten verbunden.
  5. Die Erlaubnis zur Übermittlung der Daten der Datengeber an Datennutzer lässt sich rechtlich vertretbar auch unter dem geltenden Recht konstruieren, insbesondere über einen Vertrag zwischen Data Trust und Datennutzer (Art. 6 Abs. 1 lit. b) DSGVO), aber auch über das berechnete Interesse (Art. 6 Abs. 1 lit. f) DSGVO) sowie eine Einwilligung (Art. 6 Abs. 1 lit. a) DSGVO) jeweils ggf. in Verbindung mit einer Zweckänderung nach Art. 6 Abs. 4 DSGVO. Eine Verarbeitung besonderer Kategorien personenbezogener Daten ist nur mit Einwilligung möglich (Art. 9 DSGVO).
- Sämtliche dieser Lösungen sind allerdings mit Rechtsunsicherheiten verbunden. Bei der Lösung über Art. 6 Abs. 1 lit. b) DSGVO ist umstritten, ob es überhaupt möglich ist, Datenverarbeitungen zum Leistungsgegenstand des Vertrags zu machen, wie es hier erforderlich wäre. Bei der Lösung über Art. 6 Abs. 1 lit. f) DSGVO und Art. 6 Abs. 4 DSGVO muss im Rahmen der Tatbestände eine wertende Kompatibilitätsprüfung bzw. Interessenabwägung vorgenommen werden, bei der man in sehr vielen Fällen rechtlich vertretbar auch zu einem gegenteiligen Ergebnis kommen kann. Zudem sind Behörden bei Datenübermittlungen an Dritte auf der Grundlage dieser Tatbestände traditionell skeptisch und restriktiv. Es besteht also auch hier ein rechtliches Risiko, die Datenverarbeitungen auf diese Erlaubnistatbestände zu stützen.
6. Bei der Wahrnehmung der Betroffenenrechte und bei der Geltendmachung von Abwehrbefugnissen kommt man allerdings um eine Stellvertretung nicht herum. Hierfür gelten die geschilderten Erkenntnisse.

### III. Wie kann die Lage von Data Trusts verbessert werden?

Die Lage von Data Trusts könnte auf vielen Wegen verbessert werden.

Der Optimalfall wäre es, wenn der europäische Gesetzgeber neben Verantwortlichem und Auftragsverarbeiter eine neue Rolle in der DSGVO vorsieht. Diese neue Rolle wäre nicht die betroffene Person selbst, könnte aber – jedenfalls teilweise – deren Rechte innehaben und wahrnehmen. Die gesetzliche Regelung würde die Chance eröffnen, dass die hierdurch geschaffenen Risiken für die Rechte der betroffenen Personen auf der einen Seite durch anderweitige Instrumente, wie besondere technische und organisatorische Anforderungen, ausgeglichen werden.

Eine weitere Option wäre es, in der DSGVO ausdrücklich die Möglichkeit einer Stellvertretung zu thematisieren bzw. auszubauen. Sie müsste sowohl auf Ebene der Erlaubnistatbestände, also Art. 6 DSGVO, als auch auf Ebene der Betroffenenrechte, Art. 12 ff. DSGVO, und der gerichtlichen Geltendmachung, Art. 77 -79 DSGVO, ermöglicht werden.

Regelungen zur Stellvertretung auf der Ebene der Mitgliedstaaten bergen die Gefahr, europarechtswidrig zu sein.

Schließlich würde es unter dem geltenden Recht schon helfen, einige Rechtsunsicherheiten zu beseitigen. So könnte der Europäische Datenschutzausschuss Stellung zu dem Themenkomplex der Stellvertretung unter der DSGVO nehmen oder zu der Frage, ob Verarbeitungen über Art. 6 Abs. 1 lit. b) DSGVO gerechtfertigt werden können, die selbst Leistungsgegenstand des Vertrags sind.

Berlin, 17. November 2020,  
Dr. Michael Funke, Rechtsanwalt

## Die Vereinbarkeit von Data Trusts mit der Datenschutzgrundverordnung (DSGVO)

Dr. Michael Funke, Rechtsanwalt  
November 2020

Online verfügbar unter: <https://algorithmwatch.org/data-trusts/>

Herausgeber:  
AW AlgorithmWatch gGmbH  
Linienstr. 13  
10178 Berlin

Kontakt: [info@algorithmwatch.org](mailto:info@algorithmwatch.org)

Korrektorat:  
Katrin Harlaß

Layout:  
Beate Autering  
Tiger Stangl  
[www.beworx.de](http://www.beworx.de)

Gefördert durch die



Diese Veröffentlichung ist unter einer Creative Commons  
Namensnennung 4.0 International Lizenz lizenziert  
<https://creativecommons.org/licenses/by/4.0/legalcode.de>