# VERTRAUEN STÄRKEN DURCH VERBRAUCHERFREUNDLICHE DATEN-GOVERNANCE

Stellungnahme des Verbraucherzentrale Bundesverbands zum Vorschlag der EU-Kommission für eine Verordnung über europäische Daten-Governance

12. Januar 2021


**Impressum**

*Verbraucherzentrale*
*Bundesverband e.V.*

*Team*
*Digitales und Medien*

*Rudi-Dutschke-Straße 17*
*10969 Berlin*

*digitales@vzbv.de*

Bundesverband der Verbraucherzentralen und Verbraucherverbände

Verbraucherzentrale Bundesverband e.V.

# INHALT

# I. ZUSAMMENFASSUNG

Am 25. November 2020 veröffentlichte die Europäische Kommission den Vorschlag für eine Verordnung zur europäischen Daten-Governance, der die Verarbeitung von Daten unter Beachtung der europäischen Grundwerte erleichtern soll. Der Verbraucherzentrale Bundesverband (vzbv) begrüßt im Grundsatz die Vorschläge der Europäischen Kommission, sieht aber noch Bedarf, Verbraucherinnen und Verbraucher[1] besser zu schützen. Zusammenfassend bewertet der vzbv den Verordnungsentwurf wie folgt:

- Der grundrechtliche Schutz personenbezogener Daten darf durch die Verordnung nicht unterminiert werden. Daher sollte in Artikel 1 festgelegt werden, dass die Datenschutz-Grundverordnung (DSGVO) in allen Belangen uneingeschränkt gilt.
- Zentrale Begriffe wie „Dienste für die gemeinsame Datennutzung“ und „Zwecke in allgemeinem Interesse“ sollten in Artikel 2 klar definiert werden.
- Aufgrund des nicht erkennbaren Mehrwerts der Regelungen sowie der Unterminierung datenschutzrechtlicher Grundprinzipien sollten personenbezogene Daten nicht von Kapitel 2 der Verordnung erfasst werden.
- Durch gesetzgeberische Vorgaben und die Entwicklung von Standards sollten konkrete Anforderungen an die Anonymisierung sowie an die Verwendung anonymisierter Daten definiert werden.
- Um die Risiken zu begrenzen, die mit der zentralen Rolle der Datenmittler einhergehen, und gleichzeitig das Vertrauen in diese Organisationen zu erhöhen, spricht sich der vzbv für ein obligatorisches Zertifizierungssystem für diese Dienste aus.
- Zentrale Anforderungen an Datenmittler müssen in den Normtext übernommen werden und dürfen nicht alleine in den Erwägungsgründen aufgeführt werden.
- Für datenaltruistische Organisationen sollte ein obligatorischer Genehmigungsrahmen vorgesehen werden, um ein höheres Maß an Vertrauen zu gewährleisten.
- Es sollte klargestellt werden, dass – auch im Rahmen des Datenaltruismus – bei Einwilligungen in die Verarbeitung von personenbezogenen Daten für Zwecke im allgemeinen Interesse, die keine Zwecke der wissenschaftlichen Forschung sind, stets ein festgelegter, eindeutiger und legitimer Zweck benannt werden muss.
- Die Aufsicht und die Rechtsdurchsetzung müssen wirksamer gestaltet und eine Zersplitterung der Rechtsauslegung oder gar ein Forum-Shopping verhindert werden. Außerdem müssen wirksame Sanktionen gegen Verstöße festgelegt werden.
- In Bezug auf Fragen, die eine Interpretation oder Prüfung der Einhaltung der DSGVO erfordern, sollten die für die Durchsetzung des Data Governance Acts zuständigen Behörden stets zunächst eine Stellungnahme oder einen Beschluss der gemäß der DSGVO zuständigen Aufsichtsbehörden einholen und sich nach dieser Stellungnahme oder diesem Beschluss richten müssen.
- Der europäische Dateninnovationsrat darf nicht die Stellung des europäischen Datenschutzausschusses unterminieren. Außerdem sollte der europäische Dateninnovationsrat paritätisch besetzt werden.

[1] Die im weiteren Text gewählte männliche Form bezieht sich immer zugleich auf Personen aller Geschlechter. Wir bitten um Verständnis für den weitgehenden Verzicht auf Mehrfachbezeichnungen zugunsten einer besseren Lesbarkeit des Textes.

# II. EINLEITUNG

Am 25. November 2020 veröffentlichte die Europäische Kommission einen Vorschlag für eine Verordnung zur europäischen Daten-Governance („Data Governance Act", DGA).[2] Diese Verordnung ist Teil der Europäischen Datenstrategie 2020, die darauf abzielt, die EU an die Spitze der datengestützten Gesellschaft zu bringen.[3]

Durch den DGA soll in erster Linie die Verfügbarkeit von Daten gefördert werden. Die Verordnung benennt Bedingungen für die Weiterverwendung bestimmter Kategorien von Daten, die sich im Besitz von öffentlichen Stellen in der EU befinden. Außerdem enthält sie einen Melde- und Aufsichtsrahmen für neuartige Datenmittler sowie einen Rahmen für die freiwillige Registrierung von Organisationen, die Daten für altruistische Zwecke sammeln, verarbeiten und übermitteln. Auf diese Weise soll ein Netzwerk neutraler Datenmittler entstehen, die von nationalen Behörden beaufsichtigt werden. Ziel ist es, das Vertrauen in diese Datenmittler zu stärken, die künftig unter anderem in den verschiedenen europäischen Datenräumen eingesetzt werden sollen.

Der vzbv begrüßt im Grundsatz die Vorschläge der Europäischen Kommission (EU-Kommission). Moderne Formen der Datenverarbeitung können einen großen Mehrwert für einzelne Verbraucher darstellen und zur Lösung gesellschaftlicher Herausforderungen beitragen. Auf der anderen Seite können sie aber auch Gefahren bergen, insbesondere wenn personenbezogene Daten verarbeitet werden. Einen wesentlichen Baustein, diese Risiken zu minimieren, stellt das europäische Datenschutzrecht dar – allen voran die DSGVO[4]. Sie formt das europäische Grundrecht auf den Schutz personenbezogener Daten aus und bringt es mit weiteren Grundrechten in Einklang. An ihren Prinzipien und Vorgaben müssen sich die neuen Regelungen des DGA messen lassen.

Eine verantwortungsvolle Datennutzung sowie das Grundrecht der Menschen auf den Schutz ihrer personenbezogenen Daten sind kein Widerspruch, sondern zwei Seiten derselben Medaille. Die Menschen werden der Verarbeitung ihrer Daten für das Gemeinwohl eher zustimmen, wenn es einen vertrauenswürdigen Rechtsrahmen gibt. Nur so können die Chancen der Digitalisierung realisiert, aber gleichzeitig ihre Risiken adressiert werden.

Vor diesem Hintergrund begrüßt der vzbv, dass die EU-Kommission weiterhin den Austausch mit den verschiedenen Interessengruppen sucht und bedankt sich für die Gelegenheit zur Stellungnahme.

---

[2] Vorschlag für eine Verordnung des Europäischen Parlaments und Rates über europäische Daten-Governance (Daten-Governance-Gesetz). Alle Artikel und Erwägungsgründe ohne Gesetzesangaben beziehen sich auf den DGA.

[3] Eine Europäische Datenstrategie. Mitteilung der Europäischen Kommission, COM (2020) 66 final.

[4] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

# III. POSITIONEN IM EINZELNEN

## 1. ALLGEMEINE BESTIMMUNGEN

### 1.1 Klarstellung des Verhältnisses zur DSGVO

Grundsätzlich begrüßt der vzbv das Ziel, Daten durch den DGA besser für das Gemeinwohl verfügbar zu machen. Auch aus wettbewerblichen Aspekten ist dies wünschenswert. Diesen Zielen steht der Datenschutz nicht entgegen. So sieht die DSGVO für die Verarbeitung von personenbezogenen Daten bereits eine Reihe von Erlaubnistatbeständen sowie verschiedene Privilegierungen der wissenschaftlichen Forschung vor. Darüber hinaus steckt viel Potenzial in der Verarbeitung von nicht-personenbezogen Daten, das bisher nicht ausreichend genutzt werden kann.

Daher ist es richtig, dass sich die EU-Kommission weiterhin klar zur DSGVO bekennt. Datenschutzrechtliche Grundprinzipien dürfen durch die neuen Regeln nicht unterlaufen werden: Weiterhin muss die Verarbeitung von personenbezogenen Daten auf eine geeignete Rechtsgrundlage gestellt werden. Außerdem muss bei der Verarbeitung personenbezogener Daten stets der Grundsatz gelten, dass diese Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein müssen. Dies sollte im Entwurf jedoch deutlicher herausgestellt werden.

> Der in der DSGVO festgeschriebene und grundrechtlich verankerte Schutz personenbezogener Daten darf durch den DGA nicht unterminiert werden. Zwar enthalten besonders die Erwägungsgründe viele gute Verweise auf die DSGVO, dennoch sollte in Artikel 1 festgelegt werden, dass die DSGVO in allen Belangen uneingeschränkt gilt. Beispielsweise könnte Artikel 9 (2) in Artikel 1 verschoben werden. Es ist nicht ersichtlich, warum diese Regelung auf Kapitel 3 des DGA begrenzt sein sollte.

Problematisch ist jedoch, dass der Verordnungsvorschlag an einigen Stellen nicht ausreichend zwischen personenbezogenen und nicht-personenbezogenen Daten unterscheidet. Dies führt zu Unklarheiten bei der Interpretation der Bestimmungen, die nicht zu Lasten des Datenschutzes und seiner Durchsetzung gehen dürfen. Eine deutlichere Trennung der Begrifflichkeiten und der damit verbundenen Anforderungen würde zu mehr Rechtssicherheit führen.

Darüber hinaus ist die Einbettung des Entwurfs zum Teil besorgniserregend. Beispielsweise wird in der englischen Sprachfassung der Begriff der „exploitation of data“ verwendet, was hinsichtlich personenbezogener Daten nicht angemessen ist. Bei personenbezogenen Daten handelt es sich eben nicht um ein Wirtschaftsgut, das ausgebeutet werden sollte – vielmehr ist der Schutz dieser Daten grundrechtlich verankert.

> Ferner muss bei jedem Regelungsvorschlag intensiv geprüft werden, wie das Zusammenspiel beziehungsweise die Abgrenzung zur DSGVO sichergestellt werden kann und welchen Mehrwert die Regelungen für Verbraucher und Wirtschaft bieten. Sollte dieser Mehrwert nicht ersichtlich sein, ist es besser auf die Regelungen zu

verzichten, um eine weitere Komplexitätssteigerung im Umgang mit Daten zu vermeiden.

### 1.2 Definitionen

Der vzbv bedauert, dass wesentliche Begriffe des DGA nicht definiert sind.

Insbesondere sollte in Artikel 2 eine klare Definition von „Diensten für die gemeinsame Datennutzung“ als Normadressaten erfolgen, um den Anwendungsbereich des Kapitel 3 klar einzugrenzen und um Rechtssicherheit für Unternehmen und betroffene Personen zu schaffen. Der Versuch einer Abgrenzung zu anderen Diensten alleine in den Erwägungsgründen ist nicht ausreichend. Durch schwammige Begrifflichkeiten und undeutliche Abgrenzungen zu anderen Diensten könnte ansonsten das Risiko bestehen, dass Anbieter ihre Angebote so gestalten können, dass sie zwar faktisch als Datenmittler agieren, aber dennoch nicht durch den DGA erfasst werden.

Darüber hinaus fehlt eine Definition des zentralen Begriffs der „Zwecke in allgemeinem Interesse“, für das Daten leichter verfügbar gemacht werden sollen. Der DGA spricht unter anderem von „wissenschaftliche[r] Forschung oder [der] Verbesserung öffentlicher Dienstleistungen“ – doch bei weitem nicht alle wissenschaftlichen Forschungsvorhaben liegen im allgemeinen Interesse. Ohne eine klare Definition besteht unter anderem die Gefahr, dass Verbraucher bereitwillig der Verarbeitung ihrer Daten in dem Irrglauben zustimmen, dies geschehe aus gemeinwohlorientierten Gründen während ihre Daten in Wirklichkeit kommerziell verwertet werden.

Zentrale Begriffe, wie „Dienste für die gemeinsame Datennutzung“ und „Zwecke in allgemeinem Interesse“ sollten in Artikel 2 klar definiert werden.

## 2. WEITERVERWENDUNG BESTIMMTER KATEGORIEN GESCHÜTZTER DATEN IM BESITZ ÖFFENTLICHER STELLEN

### 2.1 Kein Mehrwert für personenbezogene Daten gegenüber der DSGVO

Der vzbv erkennt den Mehrwert des Kapitels 2 hinsichtlich Datenkategorien an, die aus Gründen der geschäftlichen oder statistischen Geheimhaltung geschützt sind oder dem Schutz geistigen Eigentums Dritter unterliegen. Für diese Datenkategorien gibt es zum Teil keine mit der DSGVO vergleichbaren Regelungen, die eine Nutzung der Daten ermöglichen, aber zugleich die Rechte an diesen Daten wahren.

Hinsichtlich personenbezogener Daten ist jedoch der Mehrwert der vorgeschlagenen Regelungen nicht ersichtlich. Jegliche der hier vorgeschlagenen Datenverarbeitungsmöglichkeiten wären auch alleine auf Basis der DSGVO möglich. Auch sollten die geforderten Schutzmaßnahmen bei der Verarbeitung personenbezogener Daten schon alleine aufgrund der Vorgaben der DSGVO vorgenommen werden.

Gleichzeitig formulieren die Vorschläge einen Perspektivenwechsel hinsichtlich der Verarbeitung personenbezogener Daten, der nicht hinzunehmen ist. So muss entsprechend dem Datenschutzrecht jede Verarbeitung von personenbezogenen Daten begründet werden. Zwar formulieren die im DGA vorgeschlagenen Regelungen keine Pflicht zur Verfügungsstellung der Daten durch öffentliche Stellen. Dennoch werden

diese Stellen künftig begründen müssen, warum sie auf Anfrage von Unternehmen personenbezogene Daten nicht freigeben beziehungsweise warum sie gewisse Schutzmaßnahmen treffen.

> Aufgrund des nicht erkennbaren Mehrwerts der Regelungen sowie der Unterminierung datenschutzrechtlicher Grundprinzipien sollten personenbezogene Daten nicht von Kapitel 2 des DGA erfasst werden.

### 2.2 Regelungen für die Anonymisierung von personenbezogenen Daten

Die Weiterentwicklung von Anonymisierungstechniken ist ein wesentlicher Baustein, um die Ziele des DGA zu erreichen. Eine einwandfreie Anonymisierung stellt jedoch eine überaus anspruchsvolle Herausforderung dar, insbesondere wenn Daten über einen unbestimmten Zeithorizont mit unbestimmten Empfängern geteilt oder gar veröffentlicht werden und somit aus verschiedenen Quellen zusammengeführt werden können. Seit einigen Jahren wird verstärkt daran geforscht, wie mit entsprechenden Sicherheitskonzepten eine starke Anonymisierung erreichen werden kann, ohne dass die Analysequalität leidet. Diese Forschung an Anonymisierungsverfahren sollte verstärkt und gefördert werden.

Weiterhin hat der europäische Gesetzgeber in der DSGVO Abstand von einem absoluten Anonymisierungsbegriff genommen. Anonymisierung ist demnach nicht binär zu verstehen, vielmehr gibt es ein Spektrum verschiedener Anonymisierungsmaßnahmen, die unterschiedliche Qualitäten aufweisen und somit für verschiedene Zwecke unterschiedlich angemessen und geeignet sind. Die DSGVO gibt jedoch keine Auskunft darüber, unter welchen Umständen eine Anonymisierung als hinreichend erachtet werden kann.

> Daher bedarf es weiterer Schutzkonzepte, mit denen das Risiko einer De-Anonymisierung verringert werden kann. Durch gesetzgeberische Vorgaben und die Entwicklung von Standards sollten konkrete Anforderungen an die Anonymisierung sowie an die Verwendung anonymisierter Daten definiert werden.

Beispiele für weiterführende Schutzkonzepte finden sich im außereuropäischen Ausland. So wurde beispielsweise in Japan das Konzept der „anonymously processed information“ (API) eingeführt.[5] Für die Erstellung solcher Informationen gelten weitreichende Anforderungen, die eine De-Anonymisierung unmöglich machen oder zumindest wesentlich erschweren sollen. Auch nach der Anonymisierung müssen die Verantwortlichen weitere Sicherheitsmaßnahmen ergreifen. Darüber hinaus wurde es verboten, anonymisierte Daten mit anderen Daten zusammenzuführen, um den Personenbezug wiederherzustellen sowie im Anonymisierungsverfahren entfernte, aber noch andernorts vorhandene Merkmale zu erwerben. Ferner wurden Informationspflichten gegenüber der Öffentlichkeit eingeführt, unter anderem in Bezug auf die Kategorien von Informationen, die in den anonymisierten Daten enthalten sind.

[5] Vgl. Geminn, Christian; Laubach, Anne; Fujiwara, Shizuo: Schutz anonymisierter Daten im japanischen Datenschutzrecht (2018), in: ZD, S. 413–420, URL: https://beck-online.beck.de/Bcid/Y-300-Z-ZD-B-2018-S-413-N-1 [Zugriff: 30.12.2020].

### 2.3 Bedingungen für die Weiterverwendung

Darüber hinaus ist der Verweis auf die Pseudonymisierung in Artikel 4 (3) problematisch und sollte gelöscht werden. Denn diese Bestimmung stellt die Pseudonymisierung mit der Anonymisierung gleich, obwohl es sich dabei um verschiedene Konzepte handelt, die verschiedene datenschutzrechtliche Konsequenzen nach sich ziehen. Eine Pseudonymisierung gewährleistet keinen ausreichenden Schutz personenbezogener Daten im Kontext der Weiterverwendung dieser Daten beispielsweise für Forschung, Innovation und statistische Zwecke.

Ferner muss deutlicher werden, dass stets einer Anonymisierung Vorzug zu anderen Sicherungsmaßnahmen gegeben werden sollte, wenn personenbezogene Daten weiterverwendet werden sollen. Dieser Gedanke ist bereits in den Erwägungsgründen angelegt, er sollte jedoch auch in Artikel 5 des Normtexts übertragen werden. Gleiches sollte auch für die Datenübermittlung durch Datenmittler (Kapitel 3) sowie datenaltruistische Organisationen (Kapitel 4) gelten.

Hinsichtlich der Verarbeitung von Daten in einer sicheren Arbeitsumgebung ist unklar, welche Form die Ergebnisse einer Datenverarbeitung haben dürfen, um aus der sichereren Arbeitsumgebung entnommen zu werden. Zwar soll die öffentliche Stelle in der Lage sein, die Ergebnisse der vom Weiterverwender durchgeführten Datenverarbeitung zu überprüfen, und das Recht haben, die Verwendung der Ergebnisse zu verbieten, wenn darin Informationen enthalten sind, die die Rechte und Interessen Dritter gefährden. Angesichts der Komplexität und des Volumens der Verarbeitungen ist aber fraglich, ob öffentliche Stellen in der Lage sein werden, diese Anforderung auch in der Praxis zu erfüllen und diese zu skalieren. Vor diesem Hintergrund muss auch die Frage beantwortet werden, welche Konsequenzen öffentlichen Stellen drohen, wenn sie beispielsweise Fehleinschätzungen hinsichtlich der Sicherungsmaßnahmen treffen. Schließlich könnten solche Fehleinschätzungen massive negative Auswirkungen auf eine große Anzahl von Personen nach sich ziehen.

Auch diese Problemfelder zeigen, dass die vorgeschlagenen Regelungen bezüglich personenbezogener Daten vor allem Risiken für betroffene Personen darstellen, ohne einen echten Mehrwert gegenüber Datenverarbeitungen allein auf Basis der DSGVO zu schaffen (siehe Punkt 2.1). Dies unterstreicht erneut, dass personenbezogene Daten nicht von Kapitel 2 des DGA erfasst werden sollten.

> Sollte der europäische Gesetzgeber ungeachtet der in Punkt 2.1 angemerkten Problematik an der Weiterverwendung personenbezogener Daten festhalten, sind weitere Schärfungen der vorgeschlagenen Bedingungen zwingend erforderlich. So sollte der Begriff der Pseudonymisierung gelöscht, die Rolle der Anonymisierung gestärkt sowie die Regelungen zur Verarbeitung in sicheren Arbeitsumgebungen präzisiert werden.

## 3. ANFORDERUNGEN AN DIENSTE FÜR DIE GEMEINSAME DATENNUTZUNG

### 3.1 Anbieter von Diensten für die gemeinsame Datennutzung

Der vzbv begrüßt ausdrücklich, dass die EU-Kommission einen rechtlichen Rahmen für Datenmittler vorschlägt. Nur mit einem solchen Rahmen kann das Ziel erreicht werden,

mithilfe dieser Datenmittler die Verarbeitung beziehungsweise den Austausch von Daten zu erleichtern, ohne dabei Abstriche beim Schutz der personenbezogenen Daten der Betroffenen machen zu müssen.[6]

Solche Datenmittler könnten Verbrauchern bessere Kontrollmöglichkeiten an die Hand geben und damit das Vertrauen in die Digitalisierung und die datenverarbeitende Wirtschaft stärken. Auf der anderen Seite könnten Unternehmen auf eine größere Datenbasis mit einer besseren Datenqualität zugreifen, was wiederum die Qualität der Analysen und der Forschung verbessern würde. Nicht zuletzt würde sich die Rechtssicherheit der Datenverarbeitung erhöhen, da zum Beispiel Einwilligungen leichter entsprechend datenschutzrechtlicher Vorgaben eingeholt werden könnten.

Doch auch wenn Datenmittler die digitale Selbstbestimmung des Einzelnen fördern sollen, können von ihnen große Gefahren ausgehen. So sieht beispielsweise die Datenethikkommission der Deutschen Bundesregierung das Risiko, dass Verbraucher auf einen Weg der unbewussten oder sorglosen Fremdbestimmung geführt werden könnten. Insbesondere würde es der Idee der Datenmittler widersprechen, wenn Entscheidungen von Betroffenen an die Betreiber abgegeben oder Entscheidungen Betroffener durch diese interessenwidrig beeinflusst werden.[7] Kritisch ist in diesem Zusammenhang beispielsweise, dass im Arbeitspapier „Datenmanagement- und Datentreuhandsysteme“ der Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft im Rahmen des Digital-Gipfels 2020 das Transparency & Consent Framework des Branchenverbands IAB Europe[8] als Positivbeispiel für Einwilligungsmanagement-Dienste angeführt wird.[9] Dieses IAB-Framework widerspricht jedoch nach Ansicht Europäischer Datenschutzbeauftragter den Anforderungen der DSGVO.[10] Dies zeigt, wie wichtig eine strenge Kontrolle darüber ist, welche Organisationen als Datenmittler agieren dürfen, um Verbraucher nicht einem Risiko auszusetzen.

> Die vorgeschlagene Anmeldepflicht mit einer nachträglichen, beschwerdebasierten Kontrolle ist nicht ausreichend, um die Risiken zu begrenzen, die mit der zentralen Rolle der Datenmittler einhergehen und damit gleichzeitig das Vertrauen in diese Organisationen zu erhöhen. Der vzbv spricht sich daher für ein obligatorisches Zertifizierungssystem für Datenmittler aus, das diesen Zielen deutlich stärker Rechnung tragen würde.

[6] Vgl. Verbraucherzentrale Bundesverband: Neue Datenintermediäre - Anforderungen des vzbv an „Personal Information Management Systems“ (PIMS) und Datentreuhänder (2020). URL: https://www.vzbv.de/sites/default/files/downloads/2020/09/17/20-09-15_vzbv-positionspapier_datenintermediaere.pdf [Zugriff: 29.12.2020]

[7] Vgl. Datenethikkommission der Bundesregierung: Gutachten der Datenethikkommission (2019). S. 133, URL: https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_DE.pdf [Zugriff: 29.12.2020].

[8] IAB Europe: TCF- Transparency & Consent Framework (2018). URL: https://iabeurope.eu/transparency-consent-framework/ [Zugriff: 29.12.2020]

[9] Vgl. Fokusgruppe Datenschutz des Digital-Gipfels 2020: Datenmanagement- und Datentreuhandsysteme (2020). S. 11, URL: https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2020/p9-datenmanagement-und-datentreuhandsysteme.pdf [Zugriff: 29.12.2020].

[10] Vgl. Irish Council for Civil Liberties: Data Protection Authority investigation finds that the IAB Transparency and Consent Framework infringes the GDPR. (2020). URL: https://www.iccl.ie/human-rights/info-privacy/apd-iab-findings/ [Zugriff: 23.12.2020].

### 3.2 Bedingungen für die Erbringung von Diensten für die gemeinsame Datennutzung

Der DGA formuliert eine Reihe von Bedingungen an die Erbringung von Diensten für die gemeinsame Datennutzung. Problematisch ist jedoch, dass viele wichtige Anforderungen zwar in den Erwägungsgründen aufgeführt werden, der Normtext aber zum Teil deutlich dahinter zurückbleibt. Um Rechtssicherheit zu schaffen und ein hohes Schutzniveau sicherzustellen, sollten daher die wesentlichen Bedingungen auch direkt in den Gesetzestext (Kapitel 3) des DGA übernommen werden.

Von überragender Bedeutung ist insbesondere, dass mögliche Interessenkonflikte zwischen Datenmittlern und Datengebern ausgeschlossen werden, die trotz einer Ansiedlung der Dienste bei einer gesonderten Rechtsperson bestehen können. Ein Beispiel für mögliche Interessenkonflikte ist der Dienst Verimi, dessen Gesellschafter Unternehmen wie Allianz, Axel Springer, die Bundesdruckerei, Daimler, die Deutsche Bahn, die Deutsche Bank, die Deutsche Telekom, die Lufthansa, Samsung sowie Volkswagen Financial Services sind. Anfangs wurde der Dienst Verbrauchern gegenüber als datenschutzfreundliche Alternative zu den Single-Sign-On-Angeboten von Facebook und Google sowie als Dienst zum Einwilligungsmanagement beworben. Innerhalb der Adtech-Branche galt der Dienst jedoch als Lösung, um sich gegen die strengen Anforderungen der kommenden ePrivacy-Verordnung an eine Einwilligung für das Tracking im Internet zu wappnen.[11] Nach in der Presse zitierten Äußerungen von Verimi-Mitarbeitern soll sich dieser Ansatz zwar nicht durchgesetzt haben,[12] der Fall zeigt jedoch mögliche Interessenkonflikte auf.

> Um Interessenkonflikte zu minimieren, sollten auch im Normtext des DGA treuhänderische Pflichten der Datenmittler gegenüber den natürlichen Personen (Dateninhabern) präzise festgeschrieben werden, damit sichergestellt ist, dass diese tatsächlich im besten Interesse der Dateninhaber handeln.

Wichtig wäre außerdem, dass die Datenmittler die Dateninhaber dabei unterstützen sollten, vertrauenswürdige Datennutzer zu identifizieren. Beispielsweise sollten sie sicherstellen, dass die Daten nur entsprechend den Präferenzen der Dateninhaber und der vereinbarten Zwecke verarbeitet werden. Datenmittler sollten daher Sorgfaltsprüfungen bei den Datennutzern vornehmen müssen, bevor diese Kontakt zu Dateninhabern aufnehmen dürfen, um betrügerische Praktiken zu vermeiden.

> Datenmittler sollten Dateninhaber dabei unterstützen, vertrauenswürdige Datennutzer zu identifizieren. Hierfür ist erforderlich, dass im Normtext klargestellt wird, dass Datenmittler Sorgfaltsprüfungen bei den Datennutzern durchführen müssen.

---

[11] Vgl. Günther, Vera: Datenschutz und Datenallianzen. in: Horizont (2018), URL: https://www.horizont.net/medien/nachrichten/Datenschutz-und-Datenallianzen-Wenn-wir-nicht-reagieren-fliessen-noch-mehr-Gelder-nach-Amerika-164094 [Zugriff: 30.12.2020].

[12] Vgl. Bröckling, Marie: Eine Identität für alles: Das schwierige Geschäftsmodell von Verimi. in: Netzpolitik.org (2018), URL: https://netzpolitik.org/2018/eine-identitaet-fuer-alles-das-schwierige-geschaeftsmodell-von-verimi/ [Zugriff: 30.12.2020].

Ferner wird in der Debatte um Datenmittler oftmals angeführt, dass diese Dienste ein Instrument sein könnten, Personen die Monetarisierung ihrer personenbezogenen Daten zu ermöglichen. So macht beispielsweise der Dienst „Weople“ im Namen seiner Nutzer massenhaft bei verschiedenen Diensten und Plattformen das Recht auf Datenübertragung geltend. Die auf Weople übertragenen Daten werden anschließend durch das Unternehmen kommerzialisiert und die Nutzer an dem Gewinn beteiligt.[13] Eine Vergütung von Verbrauchern für die Verarbeitung ihrer Daten ist jedoch höchst problematisch. Aus einer grundrechtlichen Perspektive ist die Reduzierung von personenbezogenen Daten auf einen wirtschaftlichen Wert abzulehnen. Eine direkte Vergütung für Verbraucher für die Kommerzialisierung ihrer Daten setzt darüber hinaus besonders für einkommensschwache Bevölkerungsgruppen falsche Anreize und ist gesellschaftspolitisch abzulehnen.

> Daher sollte auch im Normtext klargestellt werden, dass die Geschäftsmodelle keine falschen Anreize setzen dürfen, die natürliche Personen dazu bewegen, mehr Daten für die Verarbeitung zur Verfügung zu stellen, als in ihrem Interesse liegt. Dies sollte explizit alle Modelle einschließen, bei denen Betroffene eine Vergütung für personenbezogene Daten erhalten.

### 3.3 Weitere Bedingungen für die Erbringung von Diensten für die gemeinsame Datennutzung

Über die in Punkt 3.2 genannten Bestimmungen hinaus sollten weitere Bedingungen an Datenmittler formuliert werden. So wäre notwendig festzulegen, dass Datenmittler zwingend vor Inbetriebnahme ihres Dienstes eine Datenschutz-Folgenabschätzung durchführen müssen. Außerdem sollten die Anforderungen an die Rechenschaftspflicht geschärft werden. Beispielsweise sollten Datenmittler – analog zu den Anforderungen an datenaltruistische Organisationen des Artikels 17 (4) – im Rahmen der Anmeldung ihres Dienstes belegen müssen, wie sie die Anforderungen des Kapitels 3 einhalten werden.

Vor dem Hintergrund, dass Kapitel 3 auch die Verarbeitung von nicht-personenbezogenen Daten erfasst, sollten Haftungsfragen (abseits der möglichen Verantwortung als datenverarbeitende Stelle) gesetzlich geregelt werden. Risiken, die oftmals mit digitalen Plattformen einhergehen, dürfen nicht auf Verbraucher abgewälzt werden. So muss beispielsweise die Frage geklärt werden, inwieweit auch Datenmittler haften sollten, wenn Datenempfänger betrügerische Absichten verfolgen und Daten nicht entsprechend den getroffenen Vereinbarungen verarbeiten. Denkbar wäre beispielsweise auch ein Versicherungszwang zur Absicherung von Ersatzansprüchen der Dateninhaber. Darüber hinaus sollte klargestellt werden, inwieweit Datenmittler ihre Haftung gegenüber den Dateninhabern vertraglich beschränken können.

Schließlich sollte eine potenzielle Monopolstellung einzelner Datenmittler verhindert sowie Kopplungen unterbunden werden. Dateninhabern muss stets freigestellt sein, ob sie die Dienste von Datenmittlern in Anspruch nehmen wollen – und falls ja, welche Da-

[13] Vgl. Pappalardo, Massimiliano: Data for money: App facilitating data portability now under the EDPB's scrutiny (2019), URL: https://iapp.org/news/a/data-for-money-app-facilitating-dsars-now-under-the-edpbs-scrutiny/ [Zugriff: 30.12.2020].

tenmittler sie wählen. Insbesondere sollte ausgeschlossen werden, dass etwa ein Unternehmen seine Kunden dazu verpflichtet, mit einem bestimmten Datenmittler zusammenzuarbeiten.

> In Kapitel 3 sollten weitere Bedingungen an Datenmittler formuliert werden, wie höhere Anforderungen an die Rechenschaftspflicht, die Klärung von Haftungsfragen sowie die Verhinderung von Monopolstellungen und Kopplungen.

## 4. DATENALTRUISMUS

Grundsätzlich begrüßt der vzbv die Bestrebungen der EU-Kommission, es Verbrauchern zu erleichtern, ihre Daten zum Wohl der Allgemeinheit ohne direkte Gegenleistung zur Verfügung zu stellen. Wesentlich ist dabei jedoch, dass dieses Konzept – soweit personenbezogene Daten verarbeitet werden – vollständig im Einklang mit der DSGVO stehen muss. Die vorgeschlagenen Regelungen sollten sich daher in erster Linie darauf beschränken, das Vertrauen in datenaltruistische Organisationen zu erhöhen sowie die Einholung einer DSGVO-konformen Einwilligung zu erleichtern. Nur so lässt sich erreichen, dass mehr Daten von betroffenen Personen und Unternehmen zur Verfügung gestellt werden und so ein höheres Entwicklungs- und Forschungsniveau geschaffen wird.

Es ist jedoch fraglich, ob alleine ein Eintrag in das Register der anerkannten datenaltruistischen Organisationen ausreichend ist, um das notwendige Vertrauensniveau in die entsprechenden Organisationen zu schaffen. Ähnliche Mechanismen sind zwar bereits mit Blick auf herkömmliche, gemeinnützige Spendenorganisationen etabliert – werden jedoch personenbezogene Daten gespendet, sind die potenziellen Risiken und negativen Auswirkungen für die spendenden Personen nicht überschaubar und folgenreicher. Daher sollten auch die Anforderungen an datenaltruistische Organisationen höher sein.

> Der vzbv spricht sich daher für einen obligatorischen Genehmigungsrahmen für datenaltruistische Organisationen aus, da er ein höheres Maß an Vertrauen in die Datenbereitstellung gewährleisten würde.

Als missverständlich erachtet der vzbv hingegen die Formulierungen hinsichtlich der datenschutzrechtlichen Einwilligung in Erwägungsgrund 36 sowie Erwägungsgrund 38. Diese verweisen im Kontext der Datenbereitstellung durch datenaltruistische Organisationen zu Zwecken des allgemeinen Interesses auf Erwägungsgrund 33 DSGVO. Zu beachten ist dabei jedoch, dass die Privilegierung des Erwägungsgrund 33 DSGVO auf die Verarbeitung personenbezogener Daten für Zwecke der wissenschaftlichen Forschung begrenzt ist und damit nicht jegliche Datenverarbeitungszwecke im allgemeinen Interesse einschließt.

> Dementsprechend sollte klargestellt werden, dass – auch im Rahmen des Datenaltruismus – bei Einwilligungen in die Verarbeitung von personenbezogenen Daten für Zwecke im allgemeinen Interesse, die keine Zwecke der wissenschaftlichen Forschung sind, stets ein festgelegter, eindeutiger und legitimer Zweck benannt werden muss.

Um Daten jedoch auch für weitere Zwecke im allgemeinen Interesse leichter verfügbar zu machen, sollten im Einklang mit der DSGVO weiterführende Einwilligungskonzepte, wie „dynamische Einwilligungen“, ausgebaut werden.[14] So könnte beispielweise eine betroffene Person gegenüber der datenaltruistischen Organisation festlegen, dass sie ihre Daten *grundsätzlich* für bestimmte Bereiche im allgemeinen Interesse bereitstellen würde, bei denen die Zwecke zu diesem Zeitpunkt noch nicht konkret angegeben werden können. Sollte es ein entsprechendes Interesse an einer Verarbeitung dieser Daten in dem jeweiligen Bereich geben, könnte der Betroffene über die datenaltruistische Organisation um seine Einwilligung für den konkreten Fall gebeten und mit den notwendigen fallspezifischen Informationen versorgt werden.

> Es sind daher Regelungen und Instrumente erforderlich, um das Konzept der „dynamischen Einwilligungen“ rechtlich und technisch abzubilden.

## 5. ZUSTÄNDIGE BEHÖRDEN UND VERFAHRENSVORSCHRIFTEN

Der europäische Gesetzgeber sollte dringend vermeiden, konzeptionelle Fehler der DSGVO im DGA zu wiederholen. Auch die DSGVO formuliert wichtige Anforderungen, die die Rechte der Betroffenen schützen, jedoch ist die Durchsetzung dieser Anforderungen bisher für nahezu alle Beteiligten alles andere als zufriedenstellend.[15]

Problematisch an den vorgeschlagenen Regelungen des DGA ist beispielsweise, dass für die Durchsetzung jeweils die Behörde des Mitgliedsstaats zuständig ist, in dem die Datenmittler oder datenaltruistischen Organisationen ihren Hauptsitz hat (beziehungsweise einen Vertreter benannt hat). Auch sollen die Sanktionen, die bei Verstößen gegen die Verordnung zu verhängen sind, durch die Mitgliedsstaaten erlassen werden. Gleichzeitig ist jedoch kein wirksamer Konsistenzmechanismus vorgesehen, der eine einheitliche Rechtsauslegung sicherstellen würde. Dies könnte eine Zersplitterung der Rechtsauslegung oder gar ein Forum-Shopping bewirken.

Vor diesem Hintergrund wäre es auch erforderlich, dass Dateninhaber direkt mit rechtlichen Mitteln gegen Datenmittler, datenaltruistische Organisationen sowie Datennutzer vorgehen können und ihnen dabei auch kollektive Rechtsdurchsetzungsinstrumente zur Verfügung stehen.

> Im Rahmen des weiteren Gesetzgebungsprozesses müssen die Aufsicht und die Rechtsdurchsetzung wirksamer gestaltet werden. Es gilt unbedingt, eine Zersplitterung der Rechtsauslegung oder gar ein Forum-Shopping zu verhindern. Außerdem müssen zwingend wirksame Sanktionen gegen Verstöße festgelegt werden.

---

[14] Vgl. Datenethikkommission der Bundesregierung (2019) (wie Anm. 6), S. 126.

[15] Vgl. BEUC: Commercial surveillance by Google. Long delay in GDPR complaints (2020), URL: https://www.beuc.eu/press-media/news-events/commercial-surveillance-google-long-delay-gdpr-complaints [Zugriff: 30.12.2020].

Darüber hinaus müssen dringend Situationen vermieden werden, in denen es zu abweichenden Positionen zwischen den für die Durchsetzung des DGA zuständigen Behörden sowie den Datenschutzaufsichtsbehörden kommen könnte. Für alle Fragen hinsichtlich personenbezogener Daten sowie zur Interpretation der DSGVO müssen zwingend stets die Datenschutzaufsichtsbehörden zuständig sein. Dies sollte auch für gemischte Datensets sowie für anonymisierte Daten gelten.

> Es muss klargestellt werden, dass für alle Fragen hinsichtlich personenbezogener Daten sowie zur Interpretation der DSGVO zwingend stets die Datenschutzaufsichtsbehörden zuständig sind. Insbesondere müssen die für die Durchsetzung des DGA zuständigen Behörden bei etwaigen Fragen, die eine Interpretation oder Prüfung der Einhaltung der DSGVO erfordern, stets zunächst eine Stellungnahme oder einen Beschluss der gemäß der DSGVO zuständigen Aufsichtsbehörde ersuchen und sich nach dieser Stellungnahme oder diesem Beschluss richten müssen.

## 6. EUROPÄISCHER DATENINNOVATIONSRAT

Hinsichtlich des im DGA vorgeschlagenen europäischen Dateninnovationsrats muss sichergestellt werden, dass dieser die Stellung und Positionen des europäischen Datenschutzausschusses nicht unterminiert.

So soll beispielsweise nach Erwägungsgrund 41 der Innovationsrat im Hinblick auf den Datenaltruismus die EU-Kommission in Absprache mit dem europäischen Datenschutzausschuss bei der Entwicklung des Einwilligungsformulars für Datenaltruismus unterstützen. Dies lehnt der vzbv ab. Für die Unterstützung der EU-Kommission bei der Entwicklung des Einwilligungsformulars für Datenaltruismus sollte auch weiterhin in erster Linie der europäische Datenschutzausschuss zuständig sein.

Darüber hinaus ist die Zusammensetzung des Innovationsrats unklar. Es ist nicht ersichtlich, wer als Vertreter „einschlägiger Datenräume“ gelten soll. Wie bei allen Expertengruppen der EU-Kommission sollte auch beim europäischen Dateninnovationsrat auf eine paritätische Besetzung geachtet und die Zivilgesellschaft in gleichem Maße wie die Wirtschaft berücksichtigt werden.

> Der europäische Dateninnovationsrat darf nicht die Stellung des europäischen Datenschutzausschusses unterminieren. Außerdem sollte der europäische Dateninnovationsrat paritätisch besetzt sein.