



Stellungnahme

zu den Datenstrategien der Bundesregierung und der EU-Kommission

März 2020

DATEV eG ist das Softwarehaus und der IT-Dienstleister für Steuerberater, Wirtschaftsprüfer und Rechtsanwälte sowie deren zumeist mittelständische Mandanten. Das Unternehmen zählt mit fast 8.000 Mitarbeitern zu den größten IT-Dienstleistern und Softwarehäusern in Deutschland und Europa.

Das Leistungsspektrum der DATEV reicht von mehr als 200 PC-Programmen über Cloud-Dienste wie Online-Anwendungen, Datenverarbeitung und -archivierung im Rechenzentrum bis hin zu Outsourcingleistungen sowie Sicherheitsdienstleistungen. Beratungsleistungen und Angebote zur Wissensvermittlung runden das Angebot ab.

Mit über 40.000 Mitgliedern unserer Genossenschaft erreichen wir über 2,5 Mio. KMU, deren Daten bei uns im Auftrag verarbeitet werden.

DATEV entwickelte sich konsequent zu einem international agierenden Dienstleister, der heute auch im Ausland (Italien, Österreich, Tschechien, Polen, Slowakei, Ungarn, und Spanien) unterstützt.

Die Stellungnahme der DATEV eG erfolgt ausschließlich aus dem Blickwinkel des Unternehmens als berufsständischer IT-Dienstleister, insofern wird sie unabhängig von Stellungnahmen berufsständischer Organisationen wie Kammern und Verbänden abgegeben.

EU-Transparenzregister-Nummer: 5027241291-41

Der Umgang mit Daten steht sowohl in der EU als auch in Deutschland ganz oben auf der politischen Agenda. Die EU-Kommission hat am 19.02.2020 ihre Datenstrategie vorgestellt, die des Bundes soll im Laufe des Jahres 2020 folgen.

Ziel: Digitale Souveränität

Das übergeordnete Ziel ist die **digitale Souveränität Europas**, also die Möglichkeit zur unabhängigen Selbstbestimmung in Bezug auf die „Nutzung und Gestaltung digitaler Systeme selbst, der darin erzeugten und gespeicherten Daten sowie der damit abgebildeten Prozesse“.¹

Als europäische IT-Genossenschaft wollen auch wir, DATEV eG, ein digital souveränes Europa. Um dieses Zielbild zu erreichen, sind zunächst eine differenzierte Analyse und Priorisierungen im technologischen Bereich vorzunehmen: Wo darf sich Europa in keinerlei Abhängigkeiten begeben? Hierzu gehören nach unserer Überzeugung beispielsweise Schlüsseltechnologien, hochsichere Dienste und „systemrelevante“ Plattformen, etwa solche für den Datenaustausch zwischen Unternehmen, Intermediären und Verwaltung.

In weiteren Fällen sind Nachschärfungen internationaler regulatorischer Rahmenbedingungen zur Herstellung einer größeren Rechtssicherheit und Rechtsstaatlichkeit ausreichend.

Digitale Souveränität darf jedoch in keinem Fall mit vollständiger Autarkie bzw. Abschottung verwechselt werden. In vielen Bereichen ist es aus wirtschaftlichen und rechtlichen Gründen vollkommen legitim, auch nicht-europäische Lösungen einzusetzen.

Um das Ziel der digitalen Souveränität zu erreichen, lassen sich in Bund und Europa derzeit insbesondere zwei Handlungsstränge erkennen. Zum einen soll die Verfügbarkeit von und der Zugang zu Daten verbessert werden. Zum anderen soll eine wettbewerbsfähige europäische Cloud- und Dateninfrastruktur aufgebaut werden. Die prominenteste Initiative ist hier das Gaia-X-Projekt der Bundesregierung.

Auf die folgenden Aspekte möchten wir uns in unseren Ausführungen fokussieren:

<i>Datenqualität, Standards und Rechtssicherheit als Grundvoraussetzungen</i>	2
<i>Datenzugang B2G</i>	3
<i>Datenzugang G2B – „Open Data“</i>	4
<i>B2B Datenaustausch</i>	4
<i>Anonymisierung von personenbezogenen Daten</i>	5
<i>Eine europäische Daten- und Cloudinfrastruktur</i>	6

Datenqualität, Standards und Rechtssicherheit als Grundvoraussetzungen

Bei der politischen Debatte um mehr Datenzugang ist der folgende, leider oft unbeachtete, Aspekt von entscheidender Bedeutung:

Der Zugang zu Daten ist ohne Frage eine Grundvoraussetzung für erfolgreiche, europäische datengetriebene Geschäftsmodelle. Jedoch wird in der politischen Debatte um eine regulatorische Begleitung der Datenökonomie oft übergangen, dass nicht die reine Masse an Daten zum Erfolg führt. Entscheidend ist die Qualität der Daten im Zusammenspiel mit einem konkreten Vorgehensmodell, wie die Auswertung dieser Daten einen Nutzen stiften kann. Dieses

¹ Bundesministerium für Wirtschaft und Energie (BMWi) (2019): Das Projekt GAIA-X. Eine vernetzte Dateninfrastruktur als Wiege eines vitalen, europäischen Ökosystems. BMWi, Berlin.

kann in der Wirtschaft ein Geschäftsmodell sein. In Politik und Verwaltung ist es die Verbesserung einer Verwaltungsleistung oder eine andere Maßnahme zur Unterstützung der öffentlichen Daseinsvorsorge. Der Zugang zu den Daten schließt nicht nur den physischen Zugriff auf (qualitätsgesicherte) Daten ein, sondern auch deren Beschreibung und Verknüpfbarkeit mit wiederum anderen Daten. Erst wenn diese Aspekte berücksichtigt und gelöst sind, gelingt es, aus Daten das innewohnende Wissen zu schöpfen und die skizzierten Vorteile zu erlangen.

Oberste Priorität sollte es deswegen sein, sektorübergreifend eine **hohe Datenqualität** zu gewährleisten. **Standardisierung** der Auszeichnung und Beschreibung von Daten, um diese für deren Weiterverarbeitung und Verknüpfung inhaltlich und semantisch² eindeutig zu definieren, ist dabei der Schlüssel zum Erfolg. Zum anschließenden Teilen der via Taxonomien inhaltlich abgegrenzten Daten, sind standardisierte Schnittstellen, Datenformate und Musterverträge von großer Bedeutung.

Nicht nur die Datenqualität, sondern auch regulatorische Sicherheit hinsichtlich des Umgangs mit Daten ist eine grundlegende Voraussetzung für datengetriebene Geschäftsmodelle. Gerade europäische Unternehmen sind in der Regel weniger risikobereit und eher konservativ in der Rechtsauslegung. Um europäischen Unternehmen zu helfen, wettbewerbsfähig zu sein, ist daher **Rechtssicherheit** ebenso von entscheidender Bedeutung.

Datenzugang B2G

Der von der EU-Kommission angedachte Regulierungsrahmen im Bereich Business-to-Government muss sicherstellen, dass jede Verpflichtung zur Datenherausgabe des Privatsektors an die öffentliche Hand auf ein konkretes Ziel einzahlt und nachvollziehbar begründet ist. Die Sinnhaftigkeit und Notwendigkeit muss einer Überprüfung unterzogen werden und der daraus gewonnene Nutzen für das Gemeinwohl muss den Kosten für das Unternehmen klar überwiegen.

Grundsätzlich sind freiwillige Kooperationen zum Datenaustausch zwischen Staat und Privatsektor zu bevorzugen und zu fördern. In bestimmten Situationen, wie zum Beispiel bei Pandemien, kann eine verpflichtende Herausgabe von Daten des Privatsektors gerechtfertigt sein. Jedoch sind auch in diesen Situationen freiwillige, kooperative Lösungen zu bevorzugen, da sie einfacher und schneller umzusetzen sind.

Eine **B2G-Datenfreigabe darf nur unter den folgenden Bedingungen** verpflichtend sein:

- Das Ziel, welches mit der Analyse der Daten erreicht werden soll, muss vorab klar und transparent definiert und begründet sein. Nur so hat eine verpflichtende Datenherausgabe eine legitime demokratische Grundlage.
- Datenschutzrechtliche Anforderungen müssen bei einer Datenherausgabe beachtet und Rechtssicherheit muss gewährleistet werden, dies gilt insbesondere für komplexere Konstellationen wie der Auftragsdatenverarbeitung.
- Daten, die unter das Geschäftsgeheimnis oder das Berufsgeheimnis fallen, müssen von möglichen Verpflichtungen ausgenommen sein.

² Für eine semantisch eindeutige Beschreibung bedarf es Ontologien.

- Unternehmen dürfen nicht dazu verpflichtet werden, zusätzliche Daten zu erheben. Grundsätzlich muss der bürokratische Mehraufwand so gering wie möglich gehalten und stets gegen den Nutzen abgewogen werden.
- Zusätzliche Kosten, die für Unternehmen im Rahmen eines B2G Datenaustauschs entstehen, sind von den öffentlichen Stellen zu tragen. Die dem Datenaustausch vorhergehende Datenaufbereitung ist oft ein sehr zeit- und ressourcenintensiver Prozess.
- Unternehmen dürfen nicht für die Daten, die sie teilen, haftbar gemacht werden.
- Die aus dem B2G Datenaustausch gewonnenen Daten dürfen nicht zur Strafverfolgung benutzt werden.

Datenzugang G2B – „Open Data“

Um die Verwaltung sowie die europäische Wirtschaft und Zivilgesellschaft mit Daten in ausreichender Qualität und Quantität zu versorgen, sollte der **Staat eine Vorreiterrolle** einnehmen. Bevor über weitere Datenübermittlungspflichten des Privatsektors nachgedacht wird, muss zunächst der öffentliche Sektor das Potential seiner Daten heben und diese Daten der Gesellschaft verfügbar machen. Hier besteht trotz aller bisherigen Bemühungen ein enormes Potential. Dieses gilt sowohl für die europäische Datenwirtschaft als auch für den öffentlichen Sektor selbst, der seine bereits vorhandenen Daten noch viel effektiver nutzen kann.

Es muss gewährleistet sein, dass die öffentlichen Daten aller EU-Mitgliedstaaten im **Europäischen Datenportal** auffindbar sind. Grundlage hierfür ist, dass die nationalen Datenportale, wie GovData in Deutschland, vollständig und aktuell gehalten werden. Dieses ist in Deutschland momentan noch nicht der Fall, denn nicht alle Bundesländer sind an GovData angebunden.

Die Vielzahl an (technischen) Möglichkeiten der Datenbereitstellung führt aktuell zu einem sehr heterogenen Datenangebot sowie zu einer unterschiedlichen Nutzbarkeit von Daten. Deswegen muss Open Data über semantisch eindeutig definierte Daten (Taxonomien), **standardisierte offene Datenformate und Schnittstellen** bereitgestellt werden.

B2B Datenaustausch

Ein möglicher Datenaustausch zwischen Unternehmen muss auf dem **Grundsatz der Vertragsfreiheit** beruhen. Denn jedes Unternehmen muss selbst entscheiden können, mit wem und aus welchen Gründen es Daten teilt oder nicht teilt. Bei diesen Überlegungen spielen viele Faktoren eine Rolle, wie z. B. der Datenschutz, die Wahrung von Geschäftsgeheimnissen oder eigene Geschäftsmodelle.

Um den Datenaustausch zwischen Unternehmen zu fördern, sind kooperative Datennutzungsmodelle zwischen Unternehmen der richtige Weg.

Hierfür sehen wir insbesondere in den folgenden zwei Bereichen Handlungsbedarf:

1. Es braucht **sektorspezifische Standards hinsichtlich der Datensemantik, der Datenformate und der Schnittstellen**. Dieser Standardisierungsprozess muss vorangetrieben werden. Dem Staat kommt dabei auch die Rolle zu, wenn möglich, den Weg der wirtschaftlichen Standardisierung „mitzugehen“ und einen zersplitterten Markt durch eigene Sonderwege nicht noch weiter aufzuteilen.
2. **Rechtssicherheit** zu Haftungs- und Wettbewerbsfragen sowie im Hinblick auf den Datenschutz ist eine Grundvoraussetzung für einen erfolgreichen Datenaustausch. Hier kann der Gesetzgeber mit eindeutigen Auslegungen, Leitlinien, Musterverträgen und Hinweisen auf explizite Gestaltungsspielräume, die Unternehmen auch nutzen sollen, für die nötige Klarheit sorgen.

Ein **gesetzliches Recht auf Datenzugriff zwischen Unternehmen sollte nur zur Behebung von Marktversagen und Missbrauch von Marktmacht** als letztes Mittel in Betracht gezogen werden, wie es die EU-Kommission in der EU-Datenstrategie erfreulicherweise klargestellt hat.

In diesem Zusammenhang hat sich das **PSD2-Modell** als ein grundsätzlich vielversprechender Lösungsansatz gezeigt. Die **Zweite Zahlungsdiensterichtlinie (PSD2)** ermöglicht es Dritten, auf Wunsch des Kunden, über standardisierte Schnittstellen Zugriff auf das Bankkonto des Kunden zu erhalten. Die über diese Schnittstellen zu transportierenden Daten waren außerdem bereits weitgehend semantisch eindeutig definiert. Dieser Datenzugang für Dritte geht über die Datenportabilität i. S. d. Art. 20 DSGVO hinaus und ist ein Modell, welches sich auf andere Sektoren übertragen lässt. Insbesondere für KMU, die oft in ungleichem Wettbewerb mit großen Plattformen stehen oder auf verschiedenen Plattformen nicht übergreifend agieren können, könnte dies ein geeignetes Modell sein, die Souveränität über ihre Daten zurückzugewinnen.

Dieses gilt insbesondere auch im Vergleich zu dem derzeit intensiv diskutierten Modell des **Datentreuhänders**. Der Datentreuhänder könnte zwischen die großen Plattformen und KMU geschaltet werden, um den KMU die Souveränität über ihre Daten zurückzugeben. Der Datentreuhänder soll dann die Daten der KMU gegenüber den Plattformen verwalten. Zurzeit besteht aber noch völlige Unklarheit darüber, wie das Modell eines Datentreuhänders in der Praxis konkret aussehen kann und inwieweit das Modell mit unserer heutigen Rechtslage überhaupt kompatibel ist. Insbesondere das nötige Maß an Delegierung von Einwilligungs- und Datenrechten an den Datentreuhänder scheint aus rechtlicher Perspektive schwer umsetzbar. Jedenfalls im B2B-Bereich erscheint das Modell des Datentreuhänders gerade wegen dessen Neutralität und offenen Ressourcenausstattung zu schwach, um sich gegen attraktive Geschäftsmodelle durchsetzen zu können.

Anonymisierung von personenbezogenen Daten

Datenschutz ist Teil der DNA der DATEV. Dennoch sehen wir gerade bei der Anwendung der DSGVO noch viele offene Auslegungs- und Abgrenzungsfragen. Es braucht **weitere Präzisierungen und eine einheitliche, europaweite Auslegung der DSGVO**. Insbesondere hinsichtlich der Anonymisierung von Daten besteht noch großer Handlungsbedarf, um eine Verbesserung der Datennutzung in Unternehmen und bezüglich der Zusammenführung von Daten verschiedener Anbieter zu ermöglichen. Europäische Standards für die technische Umsetzung der Anonymisierung personenbezogener Daten wären ein großer Schritt in die richtige Richtung. Die folgenden zwei Punkte wären in diesem Zusammenhang wünschenswert:

- Nach wie vor fehlt es an einer eindeutigen, EU-weiten Klarstellung, wie eine Anonymisierung von personenbezogenen Daten im Sinne der DSGVO zu interpretieren ist: Handelt es sich dabei um eine Verarbeitung nach Art. 4 Nr. 2 DSGVO? Benötigt es für die Anonymisierung von personenbezogenen Daten einer eigenen Rechtsgrundlage?
Damit die europäische Wirtschaft auch das Potential aus ihren Daten schöpfen und somit das politische Ziel der europäischen Wettbewerbsfähigkeit erreicht werden kann, braucht es hier ausgewogene Regeln. Diese sollten die Anonymisierung personenbezogener Daten praxistauglich und ohne bürokratischen Mehraufwand ermöglichen.
- Für die Anonymisierung fehlen rechtssichere Kriterien für die Bewertung, ob eine Anonymisierung vorliegt. Hier wäre ein EU-weit einheitlicher, klarer und praktisch gut anwendbarer Kriterienkatalog von großer Hilfe.³

Eine europäische Daten- und Cloudinfrastruktur

Die Schaffung einer europäischen Daten- und Cloudinfrastruktur, die mit der **Gaia-X**-Initiative der Bundesregierung erreicht werden soll, ist ein wichtiger Schritt zu mehr strategischer und organisationaler Datensouveränität in Europa.

Wir begrüßen und unterstützen diese Initiative. Wir weisen jedoch auch darauf hin, dass solche Bestrebungen nur funktionieren können, wenn sie von vornherein europäisch gedacht werden. Nur so kann sichergestellt werden, dass sich in der EU keine Parallelstrukturen bilden und die Ressourcen zielführend eingesetzt werden.

Nicht für alle unternehmerischen Bereiche stehen heute rechtlich zuverlässige und technisch ausreichend skalierbare Cloud-Lösungen zur Verfügung, um den in Europa unzweifelhaft existierenden „Datenschatz“ auch im europäischen Sinn zu heben. Oft könnte dies momentan nur mit nicht-europäischen Anbietern und Lösungen geschehen. Wenn Deutschland und Europa zur Unterstützung datengetriebener Geschäftsmodelle souveräne Lösungen entwickeln und betreiben wollen, dann gilt es zu priorisieren, in welchen Bereichen schnellstmöglich souveräne Lösungen benötigt werden. Während in Bereichen mit vergleichsweise niedriger Vertraulichkeit und niedrigen Sicherheitsniveaus auch schon heute rechtlich und technisch problemlos auf Lösungen nicht-europäischer Anbieter zurückgegriffen werden kann, gilt dies **nicht für „Hochsicherheitsbereiche“**. Ein Beispiel hierfür sind Daten, die einem Geschäfts- bzw. Steuergeheimnis unterliegen.

Gesucht sind daher ausreichend skalierbare Lösungen und Angebote in genau diesen Bereichen. Diese müssen im Idealfall die physische Speicherung von Daten in Deutschland und Europa sicherstellen, mindestens aber die rechtliche und vertragliche Zuverlässigkeit herstellen, dass Daten, die nach unserem Rechtsverständnis besonders schutzbedürftig sind, auch an anderen Orten der Welt nach unseren Standards geschützt werden. Momentan anlaufende europäische Dateninfrastrukturlösungen wie Gaia-X sollten sich zunächst darauf fokussieren, diese „Bedarflücke“ schnellstmöglich zu schließen.

³ Sowohl die Datenschutzbehörde in Österreich als auch der Bundesbeauftragte für Datenschutz und Informationsfreiheit haben sich bereits dahingehend geäußert, dass es für eine Anonymisierung ausreicht, wenn die Rekonstruktion des Personenbezugs nur mit unverhältnismäßigem Aufwand möglich wäre.