ECKPUNKTE EINER DATENSTRATEGIE DER BUNDEREGIERUNG

Kurzstellungnahme des vzbv

10. Januar 2020

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.

I. EINLEITUNG

Im November 2019 hat die Bundesregierung Eckpunkte einer Datenstrategie beschlossen. Der Verbraucherzentrale Bundesverband e.V. (vzbv) begrüßt diese Initiative sowie die grundsätzliche Ausrichtung der Eckpunkte. Moderne Formen der Datenverarbeitung können ein gewaltiger Gewinn für einzelne Verbraucherinnen und Verbraucher[1] sein und zur Lösung gesellschaftlicher Probleme beitragen. Auf der anderen Seite können sie aber auch genauso gewaltige Gefahren bergen.

Aus Sicht des vzbv sind eine verantwortungsvolle Datennutzung sowie das Recht der Menschen auf den Schutz ihrer personenbezogenen Daten kein Widerspruch, sondern zwei Seiten derselben Medaille. Daher ist es richtig, dass die Bundesregierung Datennutzung und Datenschutz nicht gegeneinander ausspielt, sondern auf der einen Seite die Chancen der Digitalisierung realisieren möchte, aber gleichzeitig ihre Risiken adressiert. Vor diesem Hintergrund begrüßt der vzbv, dass die Bundesregierung davon absieht, über die umstrittenen Begriffe des „Datenreichtums“ und der „Datensouveränität“ einen Gegenpol zum Datenschutz aufzubauen, sondern sich zu einem starken Datenschutz und der europäischen Datenschutz-Grundverordnung bekennt. Auch ist positiv, dass die Idee nicht weiterverfolgt wird, eine Art Dateneigentumsrecht einzuführen.

Um eine wirksame Strategie zu entwickeln, wäre es jedoch zielführend, eine Analyse der Stärken und Schwächen Deutschlands und Europas beim Umgang mit Daten voranzustellen. Stärken sind beispielsweise die hohen industriellen und rechtlichen Anforderungen, da diese zu einer hohen Qualität von Produkten, Angeboten und Diensten führen und Innovation freisetzen können, indem sie zu einer Differenzierung der Produkte am Markt über ihre Qualität führen.[2] Dieser Qualitätswettbewerb, die Grundlage des wirtschaftlichen Erfolgs der deutschen Wirtschaft seit der zweiten Hälfte des 20. Jahrhunderts, sollte auch im digitalen Zeitalter die Triebfeder der Wettbewerbsfähigkeit deutscher Unternehmen sein. Die industrielle Stärke Deutschlands sollte dabei auch im Umgang mit Daten in den Fokus gesetzt werden, anstatt zu versuchen, mit den Geschäftsmodellen des Silicon Valley zu konkurrieren.

Um eine so umfassende Strategie in der vorgesehenen Zeit zu formulieren, muss zwingend auf bisherigen Arbeiten aufgebaut werden. Daher ist es unerlässlich, die Erkenntnisse der Kommission Wettbewerbsrecht 4.0, des Sachverständigenrats für Verbraucherfragen sowie der Datenethikkommission, deren Bericht von allen beteiligten Stakeholdern einstimmig beschlossen wurde, bei der Formulierung der Datenstrategie umfassend zu berücksichtigen.

Zu den einzelnen Handlungsfeldern:

[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 Doppelbezeichnungen zugunsten einer besseren Lesbarkeit des Textes.

[2] Vgl. Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt: Datenschutz stärken, Innovation ermöglichen. Policy Paper (2018), URL: https://www.forum-privatheit.de/wp-content/uploads/PolicyPaper-Koalitionsvertrag-1.pdf [Zugriff: 16.12.2019].

1. DATENBEREITSTELLUNG UND DATENZUGANG VERBESSERN

Der vzbv begrüßt das Ziel der Bundesregierung, unter Beachtung der datenschutzrechtlichen Regelungen, die Bereitstellung von Daten zu verbessern und dazu die langfristige Verfügbarkeit von Daten technisch und rechtlich sicherzustellen. Von grundlegender Bedeutung ist jedoch, dass durch den Wunsch, Daten besser verfügbar zu machen, nicht das datenschutzrechtliche Grundprinzip der Datenminimierung unterlaufen wird. Weiterhin muss bei personenbezogenen Daten der Grundsatz gelten, dass ihre Verarbeitung dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein muss.

Um dieses Ziel zu erreichen, ist die Weiterentwicklung von Anonymisierungstechniken ein wesentlicher Baustein. Eine technisch einwandfreie Anonymisierung stellt im Big Data Kontext eine anspruchsvolle Herausforderung dar, insbesondere wenn die 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 jedoch verstärkt (und erfolgreich) daran geforscht, wie man mit entsprechenden Sicherheitskonzepten eine starke Anonymisierung erreichen kann, ohne dass gleichzeitig die Analysequalität leidet. Diese Forschung an Anonymisierungsverfahren sollte verstärkt und gefördert werden. Auch sollten durch gesetzgeberische Vorgaben und die Entwicklung von Standards konkrete Anforderungen an die Anonymisierung sowie an die Verwendung anonymisierter Daten definiert werden. Dies sollte um strafbewehrte Verbote der De-Anonymisierung ergänzt werden.[3]

„Personal Information Management Services“ (PIMS)[4] können eine wichtige Rolle spielen, um auf der einen Seite für eine bessere Verfügbarkeit von Daten zu sorgen, aber auch um auf der anderen Seite Menschen in die Lage zu versetzen, über die Erhebung und Weitergabe ihrer personenbezogenen Daten eine bessere Kontrolle auszuüben. Wenngleich solche Systeme primär die Selbstbestimmung des Einzelnen stärken sollen, gehen von ihnen jedoch auch erhebliche Gefahren aus. Daher sollte ein gesetzlicher Rahmen vorgegeben werden, der Zulässigkeit und Grenzen regelt, Treuepflichten normiert, konfligierende Interessen ausschließt sowie entsprechende Kontroll- und Sanktionsmöglichkeiten schafft.[5]

Auch das Instrument der Datenportabilität ist geeignet, zur besseren Bereitstellung von Daten beizutragen, indem sie Verbrauchern nicht nur mehr Kontrolle, sondern auch eine Art positives Verfügungsrecht über ihre Daten ermöglicht.[6] Dennoch ist umstritten, ob Art. 20 DSGVO lediglich Daten umfasst, die von den Betroffenen aktiv in einen Dienst eingestellt wurden oder auch solche, die von ihnen durch die Nutzung eines Dienstes oder eines Produktes generiert wurden. Um die Wirkung des Rechts auf Datenübertragung zu maximieren, muss klargestellt werden, dass das Recht alle Daten

---

[3] Vgl. Roßnagel, Alexander; Geminn, Christian: Evaluation der Datenschutz-Grundverordnung aus Verbrauchersicht. Gutachten im Auftrag des vzbv (2019), S. 96f, URL: https://www.vzbv.de/sites/default/files/downloads/2019/12/04/19-11-26_gutachten_evaluation_dsgvo.pdf [Zugriff: 05.12.2019].; Datenethikkommission der Bundesregierung: Gutachten der Datenethikkommission (2019), S. 129ff, URL: https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_DE.pdf [Zugriff: 24.10.2019]

[4] Vgl. Stiftung Datenschutz: Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen. Studie (2017), URL: https://stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/Abschluss_Studie_30032017/stiftungdatenschutz_broschuere_20170611_01.pdf [Zugriff: 06.11.2019].

[5] Vgl. Datenethikkommission der Bundesregierung (DEK) (2019) (wie Anm. 2), S. 133f.

[6] Vgl. ebd., S. 135; Roßnagel, Alexander; Geminn, Christian (2019) (wie Anm. 2), 41f

erfasst, die durch den Betroffenen verursacht wurden.[7] Außerdem sollte festgelegt werden, dass dem Betroffenen die Daten in einem interoperablen Format zur Verfügung gestellt werden müssen.

Die Gestaltung von Maßnahmen zur Erleichterung des Datenzugangs für Unternehmen sollte unter der Prämisse erfolgen, dass sie nicht zu einer Aufweichung des Datenschutzes führen. Zudem darf eine Regelung zum Datenzugang beziehungsweise eine zurzeit breit diskutierte „Pflicht zur Datenteilung“ nicht dazu führen, dass Wettbewerbsvorteile und Marktmacht großer datenverarbeitender Unternehmen und Plattformen gegenüber kleinen und mittleren Unternehmen weiter verstärkt werden.

2. EINE VERANTWORTUNGSVOLLE DATENNUTZUNG BEFÖRDERN

Ein Ziel der Strategie der Bundesregierung ist es, die verantwortungsvolle Bereitstellung und Nutzung von Daten signifikant zu steigern. Unklar ist jedoch, wie der in den Eckpunkten zentrale Begriff der „verantwortungsvollen Nutzung“ definiert ist. Der vzbv ist der Ansicht, dass eine „verantwortungsvolle Nutzung“ nicht mit einer „rechtskonformen Nutzung“ deckungsgleich sein kann. Es muss sichergestellt werden, dass eine „verantwortungsvolle Nutzung“ eine gemeinwohlorientierte Perspektive aufweist und beispielsweise eine Datennutzung ausschließt, die allein auf die Beeinflussung von Verbrauchern zu kommerziellen Zwecken ausgerichtet ist. Dementsprechend müssen die Anreize gestaltet werden.

Eng verbunden mit einer verantwortungsvollen Datennutzung ist die Frage, welche Anforderungen an algorithmenbasierte Entscheidungssysteme gestellt werden müssen. Denn diese werden künftig eine zentrale Funktion bei der Verarbeitung von Daten einnehmen. Die Datenethikkommission hat hierzu detaillierte Vorschläge gemacht, die die Bundesregierung aufgreifen sollte. In diesem Sinne sollte die Bundesregierung sich daher für eine Europäische Verordnung für algorithmische Systeme einsetzen. Diese Verordnung sollte einem risikoadaptierten Regulierungsansatz folgen mit horizontalen Regeln zur Gestaltung und Zulässigkeit von algorithmenbasierten Entscheidungssystemen und Künstlicher Intelligenz, zu Betroffenenrechten, Transparenz, Aufsichtsinstitutionen und -strukturen sowie technischen Vorgaben zur Absicherung der Rechtmäßigkeit der Systeme. Dies sollte durch sektorale Regeln weiter konkretisiert werden.[8]

Ferner kann eine verantwortungsvolle Datennutzung nur vor dem Hintergrund eines hohen IT-Sicherheitsniveaus gewährleistet werden. Jeglichen Bestrebungen die IT-Sicherheit zu schwächen, ist daher eine Absage zu erteilen. So dürfen beispielsweise Datenverarbeiter nicht dazu verpflichtet werden, Passwörter ihrer Nutzer herauszugeben oder Verschlüsselungsmaßnahmen zu umgehen. Denn jegliche Schwachstellen in der IT-Sicherheit – ganz gleich was ihre Ursache, Hintergrund oder Zielsetzung ist – können stets auch von unberechtigten Dritten ausgenutzt werden. Insofern muss sich die Bundesregierung zu einem hohen Sicherheitsniveau von Daten einschließlich stärkster Verschlüsselung bekennen. Datenschutz und Datensicherheit dürfen nicht als sicherheitspolitische und wirtschaftliche Hindernisse diskreditiert werden.

---

[7] Vgl. Regelungsvorschlag zu Art. 20 Abs. 1 DSGVO Roßnagel, Alexander; Geminn, Christian (2019) (wie Anm. 2), S. 72f.

[8] Vgl. Datenethikkommission der Bundesregierung (DEK) (2019) (wie Anm. 6), S. 180ff.

3. DATENKOMPETENZ IN DER GESELLSCHAFT ERHÖHEN

Bildung und Selbstdatenschutz sind wichtige Bausteine, um Datenkompetenz zu erhöhen. Für Verbraucher ist es beispielsweise aufgrund der mangelnden Datensicherheit bei vielen Anbietern wichtig, dass sie unterschiedliche Passwörter bei unterschiedlichen Diensten verwenden und auch sensibilisiert werden im Hinblick auf die Anforderungen an ein sicheres Passwort. Allerdings stoßen die meisten Verbraucher mit individuellen Datensicherheitsmaßnahmen schnell an ihre Grenzen. Es wäre daher – um bei dem Beispiel zu bleiben – zu kurz gesprungen, lediglich von den Nutzern individuelle Maßnahmen, wie bessere Passwörter, zu erwarten. Wichtig ist daher, dass die Verantwortung nicht allein auf die Verbraucherinnen und Verbraucher abgewälzt werden darf. Vielmehr sind auch die datenverarbeitenden Stellen und Hersteller von Produkten gefragt, Datenschutz, Datensicherheit und IT-Sicherheit durch Technikgestaltung sicherzustellen. Hier bedarf es regulatorischer Anpassungen der DSGVO und die Einführung von verpflichtenden Mindestanforderungen an die sichere Gestaltung von Produkten und Anwendungen.

4. STAAT ZUM VORREITER EINER DATENKULTUR MACHEN

Um den Staat als Vorreiter und Treiber einer verstärkten Datennutzung und Datenbereitstellung zu etablieren, sollte ein starker Fokus auf die Offenheit von Systemen und Informationen gelegt werden (Open Data / Open Source / offene Schnittstellen). Hier kommt staatlichen Stellen eine besondere Funktion zu.

Die Bundesregierung sollte daher offene Standards und Software – und damit interoperable Anwendungen – fördern. Beispielsweise könnten diese Aspekte künftig bei Vergaben der öffentlichen Hand als Vergabekriterium aufgenommen werden. Darüber hinaus sollte öffentlich finanzierte Software sowie die Daten, die im Rahmen öffentlich geförderter Projekte generiert werden, der Allgemeinheit zur Verfügung gestellt werden. So sollte beispielsweise auch ausgeschlossen werden, dass urheberrechtliche Erwägungen der Veröffentlichung von öffentlich finanzierten Gutachten und Studien entgegenstehen, um die daraus gewonnen Erkenntnisse und Daten in Dienste der Gesellschaft verwenden zu können. Dies würde Marktmacht verringern und Innovation fördern.