POSITIONSPAPIER

DIE FAMILIEN UNTERNEHMER

DIE JUNGEN UNTERNEHMER

Datensouveränität ernst nehmen
Für eine kohärente Datenpolitik, eine ausgewogene Datenschutzordnung und eine sichere, digitale Infrastruktur

Empfehlungen für die geplante Datenstrategie der Bundesregierung und die Überprüfung der EU-Datenschutzgrundverordnung (DSGVO), die am 25. Mai 2020 von der EU-Kommission vorgelegt wird

Ein zentrales Kennzeichnen der Digitalökonomie ist die Bedeutung von Daten, die zunehmend zum entscheidenden immateriellen Produktionsfaktor und zur Schlüsselressource des Geschäftserfolges werden. Daten sind die Grundlage der Industrie 4.0, einer intelligenten Verkehrssteuerung und für Vieles mehr. Der Umgang mit Daten steht hierbei in einem grundlegenden Spannungsverhältnis des Dreiecks aus Datenverwertung, Datenschutz und Wettbewerbsrecht. Insbesondere personenbezogene Daten bedürfen eines wirkungsvollen Schutzes, der jedoch wirtschaftliche Innovation und Forschungsleistungen – wie etwa im medizinischen Bereich oder zu Fragen der „Künstlichen Intelligenz“ (KI) – nicht verhindern sollte. Aus diesem Grund sollte Datenschutz nicht isoliert, sondern aus einer allgemeineren, gesamtwirtschaftlichen Perspektive gedacht werden. Und schließlich gilt es mit Hilfe des Wettbewerbsrechts die Bestreitbarkeit von (v.a. datengetriebenen) Märkten zu schützen. Im Folgenden sollen in diesem Zusammenhang Eckpunkte für eine schlüssige Datenpolitik skizziert werden.

1. Mehr Datensouveränität wagen

Datensouveränität beinhaltet, dass Unternehmen und Haushalte sicher und selbstbestimmt über ihre Daten verfügen können. Wichtige Aspekte dieser Souveränität sind Datensicherheit und die Abwehr von Datenmanipulation. Zur Cybersicherheit zählt der Schutz der Daten vor Kriminellen, ausländischen Nachrichtendiensten und Wirtschaftsspionage. Darüber hinaus müssen Daten aber auch vor staatlichem, sachgrundlosem Zugriff geschützt werden. Zwar existieren übergeordnete Interessen der Transparenz und Kriminalitätsbekämpfung, jedoch sollten die davon abgeleiteten Maßnahmen verhältnismäßig und angemessen sein. Denn auch für Unternehmer hat der Datenschutz zu gelten. Sie haben ein berechtigtes Schutzinteresse hinsichtlich Eigentümerstrukturen und Betriebsgeheimnissen gegenüber dem Staat und (ausländischen) Mitbewerbern. Das gilt im besonderen Maße für Cloud-Lösungen, bei denen Unternehmen gewiss sein müssen, dass ihre Daten sicher sind.

Die geplante „E-Evidence-Verordnung“ der EU über die grenzüberschreitende Sicherung und Herausgabe elektronischer Beweismittel in Strafsachen ist ein Beispiel für einen kaum durchdachten und unsachgemäßen Angriff auf die Datensouveränität. Auch die derzeit anstehende Umsetzung der „EU-Richtlinie zum Schutz von Whistleblowern“ in nationales Recht erfordert Augenmaß, da ansonsten womöglich zu leicht und ohne ausreichende Prüfung sensible

DIE FAMILIENUNTERNEHMER e.V.
DIE JUNGEN UNTERNEHMER
Dr. Julian Dörr
Charlottenstraße 24 | 10117 Berlin

Tel. 030 300 65-443
Fax 030 300 65-390
doerr@familienunternehmer.eu
www.familienunternehmer.eu

Betriebsinformationen an die Öffentlichkeit abfließen könnten. Das selbstbestimmte Handeln und Entscheiden im digitalen Raum erfordert zudem eine sichere, vertrauenswürdige Infrastruktur, vor allem im Bereich des Mobilfunks und der Glasfasernetze. Deutschland und Europa müssen sich also darüber Gedanken machen, wie durch strikte generelle Sicherheitsanforderungen an 5G-Netzwerkkomponenten und Zertifizierungsverfahren die digitale Souveränität nachhaltig behauptet werden kann. Zur Verringerung technologischer Abhängigkeiten sollten technische Monokulturen vermieden und Systeme stets von verschiedenen Betreibern zum Einsatz kommen – entscheidend ist zu diesem Zwecke vor allem die Unterstützung der Wettbewerbsfähigkeit europäischer Netzwerkausrüster.

2. Unternehmen die Datenverarbeitung erleichtern

Datensouveränität bedeutet ebenso die Verfügbarkeit von Daten. Unternehmen benötigen Daten für ihren täglichen Geschäftsbetrieb und zur Ermöglichung von Innovationen, da insbesondere maschinelles Lernen große Datenmengen voraussetzt (Stichwort „Big Data“). Dies wird angesichts der Konkurrenzsituation mit den USA und China, deren Firmen und Start-Ups aufgrund großer Binnenmärkte auf Millionen von Daten zugreifen und entsprechend effektiv Algorithmen trainieren können, zunehmend bedeutsam. Die von der Bundesregierung eingesetzte Datenethikkommission stellt richtigerweise fest, dass das Recht auf digitale Selbstbestimmung, also auf eine selbstbestimmte wirtschaftliche Verwertung von Daten, „auch für Unternehmen und juristische Personen“ zu gelten habe.

So wäre es beispielsweise wünschenswert, dass unpersönliche und (pseudo)anonymisierte Gesundheitsdaten für die Forschung sowie für die Entwicklung neuer Anwendungsfälle einfacher verfügbar wären – selbstverständlich unter Berücksichtigung angemessener datenschutzrechtlicher Vorgaben. Auf diese Weise könnten Patienten profitieren, indem etwa Röntgenaufnahmen durch Mustererkennung mittels Künstlicher Intelligenz zuverlässig ausgewertet werden. Anstrengungen sollte auch die öffentliche Verwaltung unternehmen, um von ihr erzeugte nicht-personenbezogene Informationsbestände wie z. B. Geodaten oder Verkehrsinformationen für die Allgemeinheit kostenlos zur Verfügung zu stellen („Open Government Data“). Die zügige Umsetzung des hierfür erdachten „Open-Data-Gesetzes“ könnte Wachstumsimpulse für neue Geschäftsmodelle geben. Inwieweit die Pflicht jedoch auf im Wettbewerb stehende kommunale Unternehmungen (wie etwa Verkehrsbetriebe) ausgeweitet werden sollte, bleibt angesichts möglicher Wettbewerbsverzerrungen noch zu diskutieren.

Für eine erfolgreiche Digitalisierung müssen somit die Bereitstellung und die langfristige Verfügbarkeit von Daten technisch und rechtlich sichergestellt werden. Hierzu ist es nicht nur notwendig, Daten auch – zumindest temporär – exklusiv nutzen zu dürfen, um Anreize für kostenintensive Investitionen in diesem Kontext zu schaffen (vergleichbar mit Patenten als zeitlich begrenztes Verwertungsrecht). Unternehmen benötigen darüber hinaus Planungssicherheit hinsichtlich der Eigentumsrechte an Daten (wem beispielsweise Fahrzeugdaten gehören).

Ebenso gilt es, den sicheren, vereinfachten und standardisierten Austausch von Daten zwischen Betrieben zu unterstützen. Unternehmen sollten von Einzelfall zu Einzelfall problemlos Datenkooperationen – unter Wahrung kartellrechtlicher Aspekte – eingehen können. Statt eine eigene Cloud-Infrastruktur zu schaffen, ist der Staat vielmehr gefordert, die Standardsetzung zu unterstützen. Durch die Zusammenarbeit privater Normungsorganisationen und wirtschaftlicher sowie staatlicher Akteure kann es gelingen, im Bereich der Digitalökonomie weltweit anerkannte Normen sowohl für den technischen Datenaustausch als auch für die Nutzungsbedingungen zu setzen und somit dem heimischen Mittelstand den Transfer von Innovationen in marktgängige Produkte zu ermöglichen. Die globale Durchsetzung solcher Normen stellt einen wichtigen Wettbewerbsvorteil dar. Strenge Regeln können sicherstellen, dass vertrauliche Daten vertraulich bleiben. Das wäre eine gute Ausgangslage für eine souveräne, selbstbestimmte Nutzung von Cloud-Diensten. Das Projekt Gaia-X des Bundeswirtschaftsministeriums, das verschiedene Cloudanbieter miteinander verknüpfen will, ist deshalb zu begrüßen.

3. EU-Datenschutzgrundverordnung anpassen

Bei privaten Haushalten liegt das Augenmerk des Datenumgangs auf dem Grundrecht der informationellen Selbstbestimmung. Demnach sollte jeder Bürger über die Preisgabe und die Verwendung seiner personenbezogenen Informationen verfügen. Diese Selbstbestimmung kann jedoch teilweise im Spannungsverhältnis zum wirtschaftlichen Verwertungsinteressen von Daten stehen: Es stellt sich die Frage nach der klugen Balance von Datenschutz und Datennutzung. Statt einer pauschalen Beantwortung ist eine differenzierte Herangehensweise erforderlich, die im Einzelnen noch weiterer Überlegungen bedarf.
Generell ist ein auf europäischer Ebene angesiedelter, einheitlicher und gemeinsamer Ansatz des Datenschutzrechts ein grundsätzlich begrüßenswerter Schritt: Er schafft EU-weit gleiche Bedingungen und ist wichtiger Baustein des digitalen EU-Binnenmarktes. Hierzu muss jedoch eine einheitliche Rechtsauslegung der DSGVO in den Mitgliedsländern angestrebt werden – bislang ist die Praxis disparat und so wird bspw. in Irland die Verordnung sehr viel laxer gehandhabt als in Deutschland. Aus gutem Grund entfaltet der europäische Ansatz als weltweit strengstes Datenschutzgesetz Vorbildcharakter. Eine sinnvoll ausgestaltete Datenschutzgrundverordnung liegt im langfristigen Interesse des Mittelstandes, auch wenn kurzfristig durchaus Kosten der Umsetzung entstehen. Aus Sicht von DIE FAMILIENUNTERNEHMER ergibt sich anlässlich der Evaluation der DSGVO jedoch die Dringlichkeit, die Verordnung in einigen Bereichen nachzubessern.

Die DSGVO soll zwar das Individuum im digitalen Raum schützen, jedoch ist die betriebliche Datenverarbeitungen nicht unter den Generalverdacht zu stellen, dass sie in der Vielzahl der Fälle gezielt Persönlichkeitsrechte zu verletzen versucht. In der neuen digitalen Wirklichkeit hinterlässt jeder Nutzer unvermeidbar eine gewisse digitale Spur, die ihm oftmals sogar einen Zugewinn an Funktionalität und Bequemlichkeit generiert. Es wäre realitätsfremd, zu versuchen, diesen Fußabdruck gänzlich zu vermeiden, vielmehr sollte es um einen bewussten Umgang mit Chancen und Risiken gehen. Insofern wäre eine ausgewogenere Einstellung gegenüber der Datennutzung angebracht.

4. Für einen zukunftsgewandten Datenschutz

Bislang müssen Nutzer gemäß der Grundidee der DSGVO allerdings in jegliche Datennutzung einwilligen (Verbot mit Erlaubnisvorbehalt). Dieser kaum an der Lebenswirklichkeit ausgerichtete Mechanismus, kann z. B. zu funktional eingeschränkten Websites und Verdruss beim Nutzer führen: Oftmals klicken sich die User etwa durch die verschiedenen Optionen, ohne die Datenschutzhinweise überhaupt zu lesen. Darüber hinaus sind ausgerechnet die großen Tech-Unternehmen aus den USA sind von dieser Regel kaum betroffen, da deren Kunden bei der erstmaligen Anmeldung mit der Zustimmung zu den allgemeinen Geschäftsbedingungen zugleich auch ihre Einwilligung zum Erfassen ihrer Netzaktivitäten geben. Während also Google oder Facebook (bzw. generell Account-basierte Modelle) bei der Datensammlung nur geringfügig eingeschränkt sind, werden die kleineren (europäischen) Wettbewerber von großen Teilen der Nutzerdaten abgeschnitten.

Dem Anwender wäre mehr geholfen, wenn eine abgestufte Herangehensweise gewählt würde. Hierzu sollte erstens verstärkt nach Datenarten differenziert und mehr Flexibilität zugelassen werden. Dazu ist u. a. eine Klarstellung nötig, wann Daten z.B. im industriellen Kontext als nicht-personenbezogen zu betrachten sind und damit nicht dem strikten Datenschutz unterliegen. Schwellenwerte nach Art der kalifornischen Regulierung zum Schutz der Privatsphäre von Dezember 2019, bei der der Datenschutz erst dann voll greift, wenn bestimmte Kriterien erfüllt werden (wie etwa einen Mindestumsatz von 25 Millionen US-Dollar), würden kleinere Organisationen und Unternehmen entlasten.

Zweitens sollte die Übertragbarkeit von Daten ausgebaut werden. Datenportabilität bedeutet, dass der Nutzer sich jederzeit entscheiden kann, die von ihm erzeugten und über ihn gesammelte Daten zu anderen Diensteanbietern zu transferieren (z. B. bei Facebook, Amazon oder WhatsApp). Die bessere Möglichkeit der Kontrolle und der Weitergabe der Daten stärkt seine Rolle und kommt dem Wettbewerb um ein möglichst hohes Datenschutzniveau zu Gute. Ferner sollte verstärkt die Pflicht zur Interoperabilität (z. B. bei Messenger-Diensten) umgesetzt werden. Hierzu müssen einheitliche Standards geschaffen und offene Schnittstellen eingerichtet werden, über die Nutzer ihre dort gespeicherten Daten einsehen können. Denkbar wäre es auch, dass solche Daten von Dritten auf Plattformen verwaltet werden, auf denen Nutzer Zugriffsrechte zu ihren Daten freigeben und entziehen können (Treuhänder-Modell).

Ein solcher souveräner Umgang mit Daten setzt natürlich eine gewisse Mündigkeit des Bürgers und die Bereitschaft voraus, sich mit der Thematik zu beschäftigen – hierzu sind auch mehr Anstrengungen in der (ökonomischen) Bildung nötig. Die Stärkung der Konsumentensouveränität hätte zudem zur Folge, dass die Datenschutzkonformität von Produkten und Dienstleistungen auf dem europäischen Markt zu eine Art Gütesiegel werden könnte. Dies eröffnet Anbietern von datenschutzkonformen Lösungen die Chance, sich auf dem Markt gegenüber datenschutzrechtlich zweifelhaften technischen Lösungen abzuheben.

DIE FAMILIENUNTERNEHMER e.V.
DIE JUNGEN UNTERNEHMER
Dr. Julian Dörr
Charlottenstraße 24 | 10117 Berlin

Tel. 030 300 65-443
Fax 030 300 65-390
doerr@familienunternehmer.eu
www.familienunternehmer.eu

5. Strikte Wahrung des Wettbewerbs

Begrenzt werden sollten die betriebliche Datensammlung und Datenverwertung jedoch, falls der Wettbewerb durch Monopolisierung eingeschränkt wird. Die spezifischen Eigenschaften der Digitalökonomie, der Netzwerkeffekt und hohe Wechselkosten (und daraus resultierender Lock-in-Effekte) führen zu einer Tendenz der „Vermachtung“: Einige Märkte, insbesondere oftmals im Bereich der Plattformökonomie (zweiseitige Märkte), kennzeichnen sich durch einige wenige marktbeherrschende Unternehmen. Dadurch werden diese Märkte wenig oder gar nicht bestreitbar. Hier ist das Wettbewerbsrecht gefragt. Es müssen Marktmachtpositionen angreifbar und Märkte kompetitiv gehalten werden.

Das deutsche und europäische Wettbewerbsrecht sollte derart gestalten werden, dass mittels fundierter Einzelfallprüfungen die Konkurrenz auf Märkten sichergestellt wird. Hierzu ist die Verpflichtung denkbar, dass marktbeherrschende Unternehmen gegen ein angemessenes Entgelt Konkurrenten Zugänge zu ihren Daten schaffen müssen. Dadurch erhielten alle Anbieter denselben Zugang zu Kunden – vergleichbar mit der Öffnung von Infrastrukturen nach der „essential facilities doctrine“. DIE FAMILIENUNTERNEHMER unterstützen diese Vorgehensweise des Referentenentwurfs zur 10. Novelle des – bereits in der Vergangenheit bewährten – „Gesetzes gegen Wettbewerbsbeschränkungen“ (GWB). Der Vorschlag des „Daten-für-alle-Gesetzes“ der SPD, Unternehmen ab einer gewissen Größe per se und marktanteilsunabhängig dazu zu zwingen, Daten zu teilen und damit Daten pauschal für alle zu öffnen – selbst wenn es sich lediglich um unbearbeitete Rohdaten handelt, schießt hingegen weit über das Ziel hinaus: Er könnte nur dazu führen, gerade deutsche Unternehmen in der Konkurrenzsituation mit internationalen Wettbewerbern schlechter zu stellen, da die heimischen Betriebe einseitig ihre Datensammlungen offenbaren müssen. Im Gegenteil: Wir benötigen ein Bekenntnis zu Dateneigentum.

6. Ordnungsrahmen für die Digitalisierung

Aus diesen Gründen benötigen Deutschland und Europa einen kohärenten Ordnungsrahmen, der ein modernes Wettbewerbsrecht, eine ausgewogene Datenschutzordnung, Ansätze zur Cybersicherheit und die Standardisierung für den sicheren und vertrauensvollen Datenaustausch umfasst und diese Komponenten aufeinander abstimmt. Ziel muss ein lebendiges Datenökosystem sein, das Datenschutz und Innovation vereint.

Deshalb fordern DIE FAMILIENUNTERNEHMER, die Chance zu nutzen, die DSGVO anlässlich der Evaluation in beschriebener Hinsicht zu verbessern sowie auf nationaler Ebene eine konsistente Datenstrategie zu konzipieren und auch zügig umzusetzen.

DIE FAMILIENUNTERNEHMER e.V.
DIE JUNGEN UNTERNEHMER
Dr. Julian Dörr
Charlottenstraße 24 | 10117 Berlin

Tel. 030 300 65-443
Fax 030 300 65-390
doerr@familienunternehmer.eu
www.familienunternehmer.eu