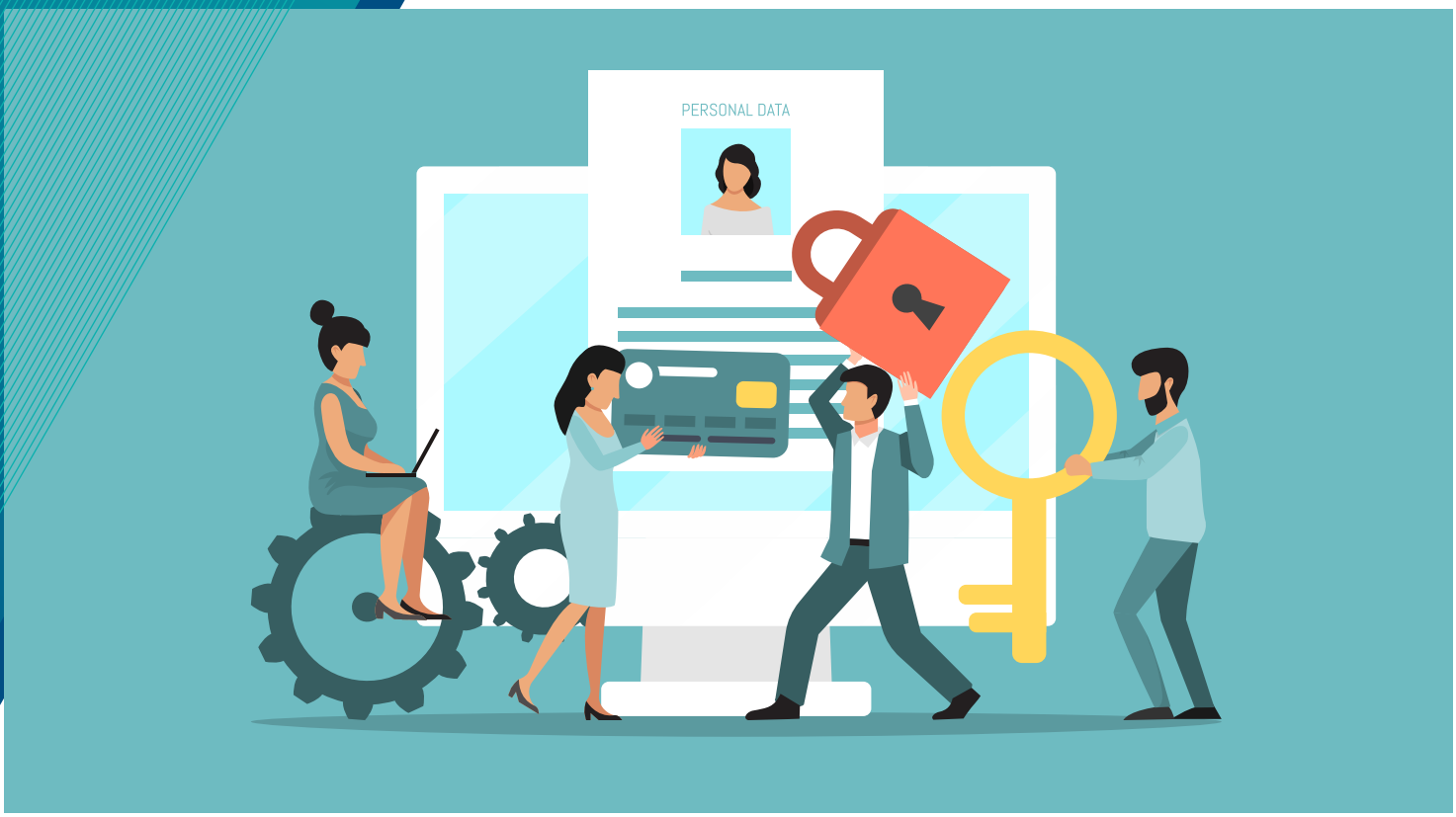
Nr. 441 / Juni 2021
Analysen & Argumente

KONRAD ADENAUER STIFTUNG



Was die DSGVO braucht

Kohärente Umsetzung und innovative Instrumente

Anne Riechert, Frederick Richter

- Der Datenschutz steht in der Kritik: Einige meinen, das Grundrecht würde in der Pandemie zu wenig eingeschränkt. Andere wiederum sehen das EU-Datenschutzrecht als Ursache für viele Probleme in der Praxis.
- Die Datenschutzgrundverordnung (DSGVO) ist ein Meilenstein, sie ist aber – wie jedes andere Gesetz auch – nicht perfekt.
- Bei der Umsetzung der DSGVO entstehen viele Unsicherheiten in der Praxis durch unterschiedliche Sichtweisen der Behörden. Die fehlende Kohärenz zwischen deutschen Datenschutzbehörden gibt Anlass für eine Neubewertung der Aufsichtsstruktur.
- Alternativ zu einer Zentralisierung der Behördenstruktur sind weitere, womöglich ebenso effektive Reformvorschläge denkbar. Infrage kommt die Verlagerung von Entscheidungskompetenzen an eine gemeinsame Geschäftsstelle der Datenschutzbehörden ebenso wie ein innerdeutsches Kohärenzverfahren nach europäischem Vorbild.
- Innovative Elemente zur Steigerung der persönlichen Datensouveränität sollten im Datenschutzrecht stärkere Berücksichtigung finden. Datenportabilität und Einwilligungsmanagement sind voranzubringen.

Inhaltsverzeichnis

Der Datenschutz und das ihn regelnde Recht sehen sich immer wieder Kritik ausgesetzt. Im medialen Diskurs wurden zuletzt Stimmen lauter, die einerseits Reformbedarf bei der Datenschutzgrundverordnung sehen und die andererseits den Datenschutz an sich zu Gunsten des allgemeinen Wohls einschränken wollen. Im Folgenden werden zunächst Aspekte herausgegriffen und näher beleuchtet, die für die Debatte besonders relevant erscheinen: Die Sicht auf den Datenschutz und der Stand des Rechts sowie dessen Durchsetzung.

Im zweiten Teil werden zwei Instrumente tiefgehender betrachtet, die mehr Aufmerksamkeit bedürfen, nämlich die Datenportabilität und die Personal Information Management Services zur möglichen Delegation von Einwilligungen.

1. Datenschutz über alles?

Wenn man auf die pandemiebedingten Freiheitsbeschränkungen zu sprechen kommt, ist eine Klage nicht weit: „Alle Grundrechte werden eingeschränkt, nur das auf Datenschutz nicht." Bei diesem Vorwurf wird zweierlei verkannt: Erstens gibt es diese Einschränkungen. So wäre es früher undenkbar gewesen, dass einmal der anonyme Besuch von Einzelhandelsgeschäften und der gesamten Gastronomie nicht mehr möglich ist. Die breit angelegte, in vielen Bereichen flächendeckende Kontaktdatenerhebung ist eine sehr konkrete Einschränkung des Datenschutzes. Weitere Einschränkungen wären denkbar und innerhalb des verfassungsrechtlichen Rahmens auch umsetzbar.[1]

Und zweitens sind nur solche Grundrechtseinschränkungen sinnvoll, die einen konkreten Nutzen bringen. Weitere Datenschutzeinschränkungen dürften nicht etwa nur deshalb stattfinden, weil andere Grundrechte ebenfalls eingeschränkt werden. In jedem Fall müssten weitere Einschränkungen des Grundrechts auf Datenschutz wirksam und verhältnismäßig sein. Die Bewegungsdaten der Bevölkerung komplett zu überwachen, um Infizierte zu lokalisieren, wäre womöglich zur Pandemiebekämpfung von Nutzen, verhältnismäßig wäre es aber nicht.

Datenschutz wird eingeschränkt wie andere Grundrechte auch.

Guter Datenschutz sollte im Idealfall so viel Schutz wie möglich für die Grundrechte und Freiheiten der Menschen bewirken und gleichzeitig nur soviel Bürokratie wie nötig mit sich bringen. Das Ziel im Datenschutz sollten Regeln sein, die verstanden werden, die befolgt werden und die durchgesetzt werden – und zwar plausibel, angemessen und konsistent. Dazu müssen die Rechtsbestimmungen nachvollziehbar und umsetzbar sein. Vor allem muss die Interpretation des einheitlichen europäischen Rechts durch die zuständigen Stellen möglichst einheitlich erfolgen und auch nach außen so kommuniziert werden. Akzeptanz ist wichtig für den Willen zur Implementierung der teils komplexen Regeln. Einheitlichkeit ist wichtig zur Vermeidung von Unsicherheiten in der Rechtspraxis.

Vor diesem Hintergrund seien im Folgenden einige Aspekte hervorgehoben, denen Aufmerksamkeit zu schenken ist, wenn es darum geht, die Wirksamkeit der EU-Datenschutzgrundverordnung zu erhöhen.

Kein Gesetz ist perfekt, auch nicht die DSGVO.

Die DSGVO ist der Meilenstein schlechthin in der Datenschutzgesetzgebung. Doch auch Meilensteine dürfen – und müssen, allein angesichts des fortschreitenden technologischen Wandels – stetig auf ihre Tauglichkeit überprüft werden. Durch eine stetige Evaluierung des Rechts, wie sie in der DSGVO vorgesehen ist, kann sichergestellt werden, dass Regulierung passgenau erfolgt. Weder dürfen Schutzlücken für die Menschen entstehen, noch sollte das Potenzial von Digitalisierung und Datenwelt ohne Not geschmälert werden.

Als Schlusspunkt der Rechtsentwicklung würde man die DSGVO nur dann betrachten dürfen, wenn zugleich die technische Entwicklung zum Stillstand käme und wenn Verhalten und Alltagsleben der Datensubjekte keinem Wandel mehr unterlägen. Da beides natürlich nicht der Fall ist, hat der europäische Gesetzgeber vorgesehen, die Regelungen des vereinheitlichten Datenschutzrechts einer dauerhaften Evaluierung zu unterwerfen. Alle vier Jahre soll die Verordnung bewertet und überprüft werden. Der Startschuss fiel 2020, vier Jahre nach der Verabschiedung des Gesetzes.

Es ist Zeit für den Beginn einer Überprüfung der DSGVO.

Einer Überprüfung müssen Reformschritte zwar nicht folgen, sie können es aber. Sollte im Rahmen der kommenden DSGVO-Evaluationen konkretes Verbesserungspotenzial ausgemacht werden, so sollten Reformen auch angegangen werden. Es wäre rechtspolitisch falsch, eine inhaltlich gebotene Modifizierung des europäischen Datenschutzrechts nur deshalb zu unterlassen, weil der Prozess, das Gesetzeswerk wieder aufzuschnüren, zu komplex und anstrengend erscheint.

2. Mehr Einheitlichkeit in der Aufsicht

Damit das vereinheitlichte europäische Datenschutzrecht seine volle Wirkung entfalten und Gesellschaft und Wirtschaft gleichermaßen zugutekommen kann, muss das Recht möglichst einheitlich aufgefasst und angewendet werden. Das erfordert bestmögliche Abstimmung unter den Aufsichtsbehörden. Eine einheitliche Sicht entsteht nicht von allein, das hat die Vergangenheit gezeigt. Daher sollte der Gesetzgeber tätig werden, um mehr Kohärenz in Deutschland zu schaffen.

In einem föderal organisierten Bundesstaat steht das einheitliche EU-Recht vor einer besonderen Herausforderung: Die Sicht auf die DSGVO und die Wahrnehmung ihres konkreten Regelungsgehalts kann sich in viele verschiedene Nuancen auffächern – wenn nämlich schlimmstenfalls jede der Datenschutzaufsichtsbehörden von Bund und Ländern eine eigene Interpretation des Gesetzestextes vornimmt. Zwar herrscht unter den Behörden keine fundamental unterschiedliche Lesart der DSGVO, doch bieten die Einzelheiten genug Spielraum für Abweichungen. Und für die Rechtspraxis und die Unternehmens-Compliance sind es oftmals bereits solche Abweichungen und Unterschiede in den Details des Datenschutzrechts, die für Unsicherheiten und zusätzlichen Aufwand sorgen können.

Manchmal liegen die datenschutzrechtlichen Wertungen zwischen den Aufsichtsbehörden der Bundesländer weit auseinander. Gelegentlich gibt es gar offenen Streit. Manche bundesweit agierenden Organisationen und Unternehmen sind daher versucht, neidisch auf EU-Mitgliedstaaten wie Frankreich zu blicken. Etwas wie die innerdeutsche „Aufsichtslandschaft“ gibt es dort nicht, denn es existiert nur eine einzige nationale Datenschutzaufsichtsbehörde. An deren Haltung zum Datenschutzrecht kann sich die Wirtschaft des gesamten Landes ein-

fach orientieren. Abweichende Meinungen unterschiedlicher Datenschutzbehörden, die für Unklarheit sorgen könnten, gibt es bei einer zentral organisierten Aufsicht nicht.

Im eigenen Land sieht es nicht so klar aus. Im vergangenen Jahr zeigte sich in Deutschland, dass wir von einer einheitlichen Auffassung zur DSGVO-Anwendung manchmal weit enfernt sind. Es ging um die Bewertung der Datenschutzkonformität von Microsoft Office 365, genauer gesagt, um die Rechtmäßigkeit der von Microsoft dazu bereitgestellten Vertragsunterlagen. Die Konferenz der Datenschutzaufsichtsbehörden von Bund und Ländern hatte dazu beschlossen, dass kein datenschutzgerechter Einsatz von MS-Office 365 möglich sei. Hierbei herrschte jedoch keine Einheitlichkeit. Der Beschluss erging mit neun gegen acht Stimmen. Und fünf der acht bei der Abstimmung unterlegenen Behörden hielten es danach sogar für angebracht, eine eigene Pressemitteilung gegen die Pressemitteilung der Datenschutzkonferenz (DSK) herauszugeben – in der sie die Bewertung der DSK als „zu undifferenziert" einstufen und sie gerade einmal „als relevante Arbeitsgrundlage" akzeptierten.[2] Derartige Uneinigkeiten werden in der Datenschutzpraxis als nicht gerade hilfreich erachtet. Sie sorgen für Unsicherheiten, welche die nötige Umsetzung dieses wichtigen Gesetzes nicht beschleunigen.

Vielstimmigkeit kann interessant sein – förderlich für eine konsistente Datenschutzdurchsetzung ist sie nicht.

Manche Unterschiede zwischen den Rechtsauffassungen der Datenschutzaufsichtsbehörden mögen eher akademischer Natur sein. Doch andere Punkte sind von hoher praktischer Relevanz. So war längere Zeit zwischen den Behörden umstritten, ob Steuerberater bezüglich der Lohnbuchhaltung datenschutzrechtlich als Auftragsverarbeiter einzuordnen seien. Die Entscheidung in dieser rechtlichen Bewertung hat praktisch hohe Relevanz, denn von ihr hängt ab, ob für Hunderttausende Steuerberaterinnen und Steuerberater datenschutzbezogene Auftragsverarbeitungsverträge hätten abgeschlossen werden müssen. Doch obwohl sowohl das Steuerrecht als auch das Berufsrecht der Steuerberater bundesweit einheitlich geregelt sind und das Recht zur Auftragsverarbeitung personenbezogener Daten sogar europaweit, zog sich bei der Bewertung ein Riss durch die Reihe der Landesbehörden, und es war keine Einigung in Sicht. Auch die Stiftung Datenschutz versuchte zu vermitteln und versammelte Landesbehörden sowie Interessenvertretung und Kammer der Steuerberater an ihrem runden Tisch. Doch war es erst eine gesetzgeberische Klarstellung, die den jahrelangen Dissens in der Bewertung abräumte. Es wurde im Steuerberatungsgesetz festgelegt, dass die Verarbeitung personenbezogener Daten durch Steuerberaterinnen und Steuerberater immer weisungsfrei ist und daher keine (immer weisungsgebundene) Auftragsverarbeitung darstellen könne. Mit dieser Klarstellung wurde immenser bürokratischer Aufwand vermieden. Das Beispiel zeigt, wie fehlende Einheitlichkeit in der Datenschutzaufsicht ein bremsender Faktor sein kann.

Die fehlende Kohärenz im innerdeutschen Datenschutz gibt Anlass für eine Neubewertung der Aufsichtsstruktur im Datenschutz. Am Ende dieser Prüfung muss nicht eine generelle Neuordnung der Datenschutzaufsicht in Deutschland oder eine formelle Zentralisierung der Behördenstruktur stehen. Unbedingtes Ziel sollte jedoch eine inhaltliche Vereinheitlichung sein – ganz im Geiste der erfolgten europäischen Rechtsangleichung.

Als Vorteil der überkommenen Zuständigkeitsverteilung (Datenaufsicht über die Wirtschaft durch die Länder) wird meist die Bürgernähe genannt. Und natürlich brauchen die von der DSGVO in ihren Freiheitsrechten zu schützenden Bürgerinnen und Bürger eine direkt ansprechbare und leicht erreichbare Datenschutzaufsicht. Eine gute Erreichbarkeit mag sich auf Bundes- wie auf Landesebene gleichermaßen herstellen lassen. Auch dürften persönliche Besuche in Behördengebäuden nicht mehr den Regelfall darstellen. Bei Fernkontakt wird es für viele Beschwerdewillige kaum Unterschied machen, ob sie sich telefonisch oder per E-Mail an eine Behörde in der Landeshauptstadt oder in der Bundeshauptstadt wenden.

Alternative Reformvorschläge zu einer Zentralisierung gibt es mittlerweile mehrere:

a) Nach einem Vorschlag der Datenethikkommission der Bundesregierung könnte die Aufsicht über den nicht öffentlichen Bereich, also die Unternehmen, dem Bundesbeauftragten übertragen werden.[3] Im Zuge seiner Zuständigkeit zur Regelung des Rechts der Wirtschaft könnte der Bund autonom die Kompetenz der wirtschaftsbezogenen Datenschutzaufsicht auf den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit übertragen. Dieser könnte durch verschiedene Außenstellen die Präsenz der Datenschutzaufsicht auch in der Fläche weiterhin sicherstellen.

b) Einer anderen Ansicht zufolge könnte die Datenschutzaufsicht der oder des Bundesbeauftragten auf solche Unternehmen ausgeweitet werden, die im Dax oder MDax gelistet sind oder eine ähnliche Kapitalisierung haben. Für alle übrigen Unternehmen wären weiterhin die Landesbehörden zuständig.[4] Dies könnte zwar die Schlagkraft der Rechtsdurchsetzung gegenüber großen Akteurinnen und Akteuren verbessern, könnte aber gleichzeitig bedeuten, dass im Mittelstand die problematische Vielstimmigkeit auf Seiten der Datenschutzaufsicht bestehen bleibt. Selbst wenn man dem entgegenhält, dass sich ein Mittelständler doch einfach nur an die für ihn maßgebliche Sicht der Aufsicht seines eigenen Bundeslandes halten möge, so ändert dies nichts am Grundproblem: Wenn das vollharmonisierte EU-Datenschutzrecht etwa von der hessischen Aufsicht in Wiesbaden anders interpretiert wird als von der rheinland-pfälzischen Aufsicht in Mainz, befördert dies das allgemeine Verständnis der DSGVO nicht.

Orientierung an bewährten Strukturen des Rundfunkrechts: gemeinsame Geschäftsstelle mit Entscheidungskompetenz.

c) In eine andere Richtung zielt der Ansatz, die bestehende Aufsichtsstruktur nicht grundlegend zu verändern, sondern durch eine zusätzliche Einrichtung zu ergänzen. Dies würde eine Parallele zur Rundfunkaufsicht ziehen und sich an deren Struktur orientieren. Bei den Aufsichtsbehörden für den privaten Rundfunk stellt sich wie beim Datenschutz die Frage: Wie kann eine Aufsicht organisiert werden, die zwar aus sachlichen Gründen bundeseinheitlich erfolgen muss – der Rundfunk mache ebenso wie die Datenströme nicht an Bundeslandgrenzen halt – aber dennoch aus föderalen Erwägungen bei den Ländern verbleiben soll? Die Landesgesetzgeber haben auf diese Fragen mit einer Vereinheitlichung des Landesrechts geantwortet, der Delegation gewisser Entscheidungskompetenzen und mit der Errichtung einer gemeinsamen Geschäftsstelle. Während die Rechtsvereinheitlichung im Datenschutz durch die EU-weite Konsolidierung nur noch in Randbereichen eine Rolle spielt (beispielsweise im Presserecht), wäre die Möglichkeit zur Kompetenzabgabe von der Ebene des jeweils einzelnen Bundeslandes auf eine höhere Ebene der Datenschutzkonferenz eine interessante Perspektive. Analog zu den im Rundfunkrecht bestehenden Kommissionen könnten die DSK-Arbeitskreise ermächtigt werden, für alle Bundesländer verbindlichen Rechtsauslegungen festzulegen. In einer gemeinsamen Geschäftsstelle der Landesaufsichten würden die Positionen ausgearbeitet. Im Effekt erarbeiteten die Länder in diesem Modell bundeseinheitliche Regelungen, ohne Kompetenzen an eine Bundesbehörde abgeben zu müssen.

Von Europa lernen – mit einem eigenen deutschen Kohärenzverfahren

d) Ein anderer Ansatz zur Stärkung der föderalen Entscheidungsfindung sieht ein Kohärenzverfahren für die Datenschutzkonferenz der Landesbeauftragten und des Bundesbeauftragten vor – ganz nach dem Vorbild des bereits nach der DSGVO für die europäische Ebene vorgesehenen Kohärenzverfahrens.[5] Ein Bund-Länder-Staatsvertrag könnte die Koordinationsmechanismen der DSGVO auf Deutschland übertragen. In strittigen Fragen träfe die Datenschutzkonferenz von Bund und Ländern verbindliche Mehrheitsentscheidungen – unter Umständen sogar gegen das Votum der federführenden Landesbehörde. Ein solches Modell ist der deutschen Aufsicht nicht völlig fremd, denn

das die DSGVO begleitende Bundesdatenschutzgesetz sieht bereits ein Kohärenzverfahren vor, und zwar für die Vorbereitung von Beschlüssen des Europäischen Datenschutzausschusses. Bei einer Übertragung des EU-Kohärenzverfahrens auf Deutschland könnte festgelegt werden, dass strittige Fälle, die mehrere Bundesländer betreffen, der Datenschutzkonferenz zur verbindlichen Beschlussfassung vorgelegt werden müssen. Feste Fristen für die Befassung und Entscheidung der DSK könnten eine zeitnahe Befassung der Datenschutzaufsicht mit dringenden und kontroversen Themen sicherstellen. Auf diese Weise ließe sich vermeiden, dass „unwillige oder unfähige Datenschutzbehörden" Entscheidungen verhindern oder verschleppen. Mit diesem Modell ließe sich sowohl Kohärenz als auch mehr Tempo bewirken.

3. Mehr Selbstbestimmung durch mehr Datenübertragbarkeit

In der Praxis gibt es bisher weitgehend keine Erfahrungswerte zum Umgang mit dem „Recht auf Datenübertragbarkeit" aus Art. 20 DSGVO. Insgesamt besteht jedoch nach wie vor ein großer Bedarf an einer umfassenden Analyse dahingehend, wie sich das bestehende Portabilitätsrecht sowohl auf den Markt als auch auf die Gesellschaft und den Einzelnen auswirkt.[6] Welchen technischen Herausforderungen muss begegnet werden und welches wirtschaftliche Potenzial steckt im Recht auf Datenübertragbarkeit? Eine wichtige Frage ist gleichwohl, wie sich das Recht auf Datenübertragbarkeit als datenschutzrechtliches Kontrollrecht mit der Idee eines freien Datenflusses verbinden lässt, und die Rechte der Betroffenen dennoch gewahrt werden können. Gemäß dem Wortlaut von Art. 20 DSGVO ermöglicht dieses Recht, personenbezogene Daten, die Betroffene einem Dienstleister entweder aufgrund ihrer Einwilligung oder aufgrund eines Vertrages zur Verfügung gestellt haben, zu einem anderen Dienstleister ohne Behinderung zu übermitteln oder sogar die Übermittlung der Daten an einen anderen Dienstleister zu verlangen. Mit Blick auf die Übermittlung zu einem weiteren Anbieter ist zu berücksichtigen, dass damit keine automatische Löschung der Daten beim ursprünglichen Dienstleister verbunden ist, sondern dieses (Kontroll-)Recht der DSGVO vielmehr gesondert geltend gemacht werden muss. Daher hat ebenso der ursprüngliche Dienstleister weiterhin (in den Grenzen der DSGVO) das Recht zur Verarbeitung der Daten.

Recht auch Datenportabilität – wie weit reicht es, was umfasst es konkret?

In der Praxis befassen sich bereits verschiedene Initiativen mit Fragen zur Datenportabilität,[9] wie etwa das Data Transfer Project,[10] die Data Portability Cooperation unterschiedlicher Telekommunikationsanbieter[11] oder die Initiative New Governance[12] – letztere mit dem Fokus auf einen branchen- und sektorübergreifenden Datentransfer (Flow of Data). Die Zusammenarbeit innerhalb dieser Projekte konzentriert sich unter anderem auf die Prüfung technischer Voraussetzungen, da insbesondere die Interoperabilität der Dienste als technische Voraussetzung für die Umsetzung der Datenportabilität grundlegend ist. Daher hat die Artikel-29-Datenschutzgruppe (Vorgängerinstitution zum Europäischen Datenschutzausschuss).[13] Branchenvertreter und Verbände in den von ihr veröffentlichten Leitlinien zur Datenportabilität bereits dazu aufgefordert, gemeinsame Formate zu entwickeln[14] und insgesamt eine weite Auslegung der Regelung vorgenommen. So sollen vom Recht auf Datenübertragbarkeit ebenso Observed Data umfasst sein, also nicht nur Vertragsdaten, die ein Nutzer oder eine Nutzerin aktiv bereitstellt, sondern ebenso Daten, die aufgrund der Inanspruchnahme eines Dienstes erzeugt werden (z. B. Suchverlauf, Standortdaten oder die von einem Trackinggerät aufgezeichnete Herzfrequenz) sowie Metadaten.[15] Hierfür bedarf es technischer Standards. Ansonsten würde dieses Recht in der Praxis leerlaufen. Allerdings scheint es in diesem Zusammenhang derzeit einen Widerspruch zu geben: Einerseits wird auf EU-Ebene darauf verwiesen, dass eine Interoperabilitätspflicht ebenso innovationshemmend sein kann. Andererseits können jedoch nur gemeinsame Standards dabei unterstützen, die Portabilität von Daten sicherzustellen. Aus diesem Grund könnte sich die weitere

Forschung dahingehend empfehlen, welche Dienste und Branchen durch erleichterte Datenportabilität profitieren könnten und welche Maßnahmen darüber hinausgehend erforderlich wären, um gerade auch die Macht von marktbeherrschenden Unternehmen zu brechen, ohne dass in diesem Bereich die befürchtete innovationshemmende Wirkung eintritt. So könnten standardisierte Datenformate ebenso den Zugang zu Daten verbessern.[16]

Eine Pflicht zur Interoperabilität als Turbo für die Praxis?

Um die Möglichkeiten und Grenzen einer Datenportabilität vollständig erfassen zu können, könnte außerdem ein Blick auf die Historie dieses in der DSGVO genannten Rechts hilfreich sein. Ursprünglich war das Recht auf Datenübertragbarkeit zum einen als Verbesserung des Auskunftsrechts ausgestaltet, und die betroffene Person hatte bei einer elektronischen Verarbeitung einen Anspruch darauf, die Daten, die Gegenstand einer Auskunft waren, als Kopie in einem gängigen elektronischen Format zu erhalten.[17] Zum anderen wurde bei einem Anbieterwechsel der Fokus auf soziale Netzwerke gelegt.[18] So hatte der europäische Gesetzgeber geplant, die Monopolstellung von sozialen Netzwerken durch Netzwerkeffekte aufzuweichen und den Wechsel zu datenschutzfreundlichen Technologien zu ermöglichen.[19] Dieser wettbewerbsrechtliche Charakter, der dazu führt, dass das Recht auf Datenübertragbarkeit oftmals als Fremdkörper im Datenschutzrecht eingestuft wird, wurde zuletzt durch die oben genannten Leitlinien der Datenschutzaufsichtsbehörden zum Recht auf Datenübertragbarkeit bestätigt. Diese verweisen darauf, dass die direkte Übermittlung personenbezogener Daten von einem Verantwortlichen an einen anderen ein wichtiges Werkzeug zur Unterstützung des freien Verkehrs personenbezogener Daten in der EU und zur Förderung des Wettbewerbs zwischen Verantwortlichen sei. Es erleichtere den Wechsel zwischen verschiedenen Dienstanbietern und werde daher die Entwicklung neuer Dienste im Kontext der Strategie für einen digitalen Binnenmarkt fördern.[20] Daher können als Stichworte der „freie Datenfluss“ sowie „Datensouveränität“ genannt werden.[21] Zu berücksichtigen ist außerdem, dass die ursprüngliche Intention zwar der Wechsel zu einem datenschutzfreundlichen Netzwerk war, aber das Recht auf Datenübertragbarkeit ebenso den Wechsel zu jedem Dienst ermöglicht (der durchaus auch datenschutzunfreundlich sein könnte). Der ausschließliche Blick auf soziale Netzwerke wird zudem durch die Rechte Dritter erschwert, die bei einem Wechsel nicht verletzt werden dürfen.[22]

Portabilitätsrechte: Ermöglichung persönlicher Datenkontrolle

Insgesamt darf das Recht auf Datenübertragbarkeit aus datenschutzrechtlicher Sicht nicht soweit aufgeweicht werden, dass es letztendlich für Anbieter als Legitimationsgrundlage dient, Daten für eigene Zwecke zu erlangen. Das Recht auf Datenübertragbarkeit ist ein Kontrollrecht für Betroffene, keine Rechtsgrundlage für Dienstleister. Es wäre daher verfehlt, ausschließlich den Servicegedanken beim Recht auf Datenübertragbarkeit in den Vordergrund zu rücken, indem Nutzerinnen und Nutzer seitens der Verantwortlichen durch die Bereitstellung bequemer Lösungen dazu „überredet“ werden, ihre Daten preiszugeben (Nudging) – auch wenn in der Praxis die Grenzen verschwimmen können. Dennoch sollten weiterhin die Möglichkeiten untersucht werden, wie Datenportabilität einerseits mit dem Begriff der „Datensouveränität“ zusammenspielt und diese gestärkt werden kann, und ob andererseits durch das Recht auf Datenübertragbarkeit der Zugang zu Daten erleichtert werden könnte. Dabei sollten auch die Möglichkeiten der Übermittlung von Echtzeitdaten näher untersucht werden.

Die Stärkung von „digitaler Souveränität“ kann dabei ebenso eine Rolle spielen:[24] Wird die Datenportabilität für Betroffene erleichtert und werden in diesem Zusammenhang Maßnahmen geprüft, die die Datenübertragung von marktbeherrschenden Unternehmen auf Unternehmen mit Sitz in Deutschland oder Europa begünstigen können, kann gleichermaßen die Unabhängigkeit sowohl von Technologien aus Drittstaaten als auch die Durchsetzung eigener Werte- und Rechtsvorstellungen gefördert werden. Das Recht auf Datenübertragbarkeit stellt ebenso ein wettbewerbliches Instrument dar, um den freien Fluss von Daten in der

Europäischen Union zu unterstützen. Diese Intention der Datenportabilität sollte daher auch zukünftig näher untersucht werden, um den Datenaustausch zu fördern. Davon können gleichermaßen Forschung sowie Innovation profitieren. So könnten verfahrenstechnische und rechtliche Hürden, gerade mit Blick auf personenbezogene Daten, aber ebenso Geschäftsgeheimnisse, durch die Förderung neutraler (branchen- oder sektorspezifischer) Intermediäre als wichtige Eckpfeiler überwunden werden.

Von mehr Datenportabilität und mehr Datenaustausch können Forschung und Innovation profitieren

Gemeinsame Datenräume können Portabilität und Portierung von Daten deutlich erleichtern. Entsprechende Orientierung für die Verbesserung gemeinsamer Datennutzung und für einen Rahmen eines Datenaustausches enthält der Vorschlag über europäische Data-Governance. Es empfiehlt sich daher die Untersuchung sowohl konkreter praxisrelevanter Use Cases als auch flankierend die institutionelle Ausgestaltung solcher Intermediäre, ihrer technischen Voraussetzungen sowie die jeweiligen vertraglichen Bedingungen der Datennutzung.

4. Mehr Selbstbestimmung durch weniger Einwilligungsanfragen

Die Auseinandersetzung mit Personal Information Management Systems oder Personal Information Management Services (abgekürzt jeweils: PIMS) mit Diensten unter Einsatz von Privacy Enhancing Technology (PET) oder mit Einwilligungsmanagement-Systemen (im anglo-amerikanischen Raum teilweise Privacy Management Tools, PMT) befindet sich noch am Anfang. Eine allgemeine Definition besteht nicht. Die Begrifflichkeit ist rechtlich nicht geschützt und wird für unterschiedliche daten- und datenschutzbezogene Dienstleistungen genutzt. Die verschiedenen Dienste und Systeme lassen sich übergreifend beschreiben als eine technologiegestützte Anwendung zum Aufbau von Ökosystemen, mit deren Hilfe Personen in die Lage versetzt werden, die Sammlung und Verarbeitung, Verbreitung und Austausch ihrer persönlichen Daten besser zu überblicken und zu steuern. Die Zielstellung des PIMS-Ansatzes wird in der Gesetzesbegründung auch als Ziel der DSGVO benannt („Natürliche Personen sollten die Kontrolle über ihre eigenen Daten besitzen." Erwägungsgrund 7, Satz 2 DSGVO).

Auf europäischer Ebene, ausgehend von Finnland und der Initiative MyData, wird dem schon länger Beachtung geschenkt. Im Jahre 2017 wurden in Deutschland in einer Studie die technischen, rechtlichen und ökonomischen Herausforderungen von PIMS untersucht.[25] Dargestellt wurden unter anderem die Ziele von PIMS, wobei der Fokus stets auf den Kontrollmöglichkeiten von betroffenen Personen über ihre personenbezogenen Daten lag. In einem weiten Verständnis kann diese Kontrollmöglichkeit ebenso durch Erleichterung von Auskunftsersuchen oder Verbesserung von Informationsrechten, durch Aufheben von Informationsasymmetrien, erreicht werden: „Transparenz über die Datenverarbeitung!" So ist Nutzern und Nutzerinnen beispielsweise oftmals nicht bewusst, auf welche persönlichen Daten, die auf dem jeweiligen Endgerät gespeichert sind, eine installierte App zugreift – geschweige denn, dass überhaupt ein Zugriff erfolgt. Aber unabhängig davon, ob seitens der Betroffenen eine bewusste oder unbewusste Entscheidung über die Preisgabe von persönlichen Daten erfolgt ist, muss diese auch wieder zurückgenommen werden können. In diesem Sinne unterstützte ein in der Studie untersuchter Dienst bei der Deinstallation solcher Apps. Ebenso hatten weitere Dienste die Verbesserung der datenschutzrechtlichen Kontrollrechte zum Ziel (beispielsweise durch Erleichterung von automatisch generierten Auskunftsersuchen, verbesserte grafische Darstellung von Informationen über die jeweilige Datenverarbeitung, Bereitstellen einer Linksammlung zu den Privatsphäreeinstellungen unterschiedlicher Anbieter oder lokalen Verwaltungsmöglichkeiten persönlicher Daten auf dem eigenen Endgerät, wenn diese bei unterschiedlichen Anbietern gespeichert sind).[26]

Mehr Datenkontrolle für eine nutzerzentrierte Ausgestaltung der Datenökonomie

Vom reinen Einwilligungsmanagement bis zum echten Einwilligungsassistenten – PIMS bieten viele Chancen

Die Europäische Kommission beschreibt PIMS allerdings in einem engeren Verständnis, und zwar als Möglichkeit der Nutzer und Nutzerinnen, personenbezogene Daten in sicheren, lokalen oder Online-Speichersystemen zu verwalten und sie zu teilen, wenn sie dies wünschen. Die Vorstellung ist, dass Anbieter von Onlinediensten und Werbetreibende mit PIMS interagieren müssen, wenn sie beabsichtigen, die Daten natürlicher Personen zu verarbeiten und dadurch letztendlich neue Geschäftsmodelle entstehen können. Dies könnte auch als „Einwilligungsassistent" oder als „Personal Data Wallet" bezeichnet werden.[28] Insgesamt könnte ein Dienst dergestalt entwickelt werden, dass Datenschutzhinweise der Empfänger in eine maschinenlesbare Form übersetzt und die darin enthaltenen Angaben in Form einer Liste zusammengefasst werden können, damit die betroffene Person in die Verarbeitung der dort aufgezählten Daten, Zwecke und Empfänger detailliert einwilligen kann.[29] Die datenschutzrechtliche Herausforderung, die bei einer solchen Vorgehensweise stets gelöst werden muss, ist die Sicherstellung einer informierten Einwilligung im Sinne der DSGVO für einen oder mehrere bestimmte Zwecke, die so präzise wie möglich festgelegt werden müssen. Eine pauschale Einwilligung ist unwirksam und der Zweck der Verarbeitung muss bestimmt und eindeutig sein. Allerdings hat nun eine Studie von Conpolicy aus dem Jahre 2020 gezeigt, dass zumindest im bilateralen Austausch, also zwischen einem Nutzer oder einer Nutzerin und einem Unternehmen im Rahmen eines laufenden Vertragsverhältnisses, ein Einwilligungskonzept funktioniert und praktikabel ist: Es gibt technische sowie gestalterische Möglichkeiten, datenschutzfreundliche Voreinstellungen entsprechend der Vorgaben der DSGVO rechtskonform festzulegen, und Verbraucher sowie Verbraucherinnen befürworten gemäß dieser Studie überwiegend differenzierte Einwilligungen und datensparsame Voreinstellungen.[30] Um jedoch den Zugang zu Daten für wirtschaftliche und gesellschaftliche Zwecke sicherzustellen und gleichzeitig den betroffenen Personen mehr Kontrolle über „ihre" Daten zu geben, bedarf es der Erforschung und praktischen Erprobung, inwieweit durch Einwilligung die Datennutzung nicht nur in einem laufenden Vertragsverhältnis, sondern auch zwischen unterschiedlichen Dienstanbietern ermöglicht werden kann. Dies kann außerdem sowohl zur Verbesserung der „Datensouveränität" als auch zur Stärkung der „digitalen Souveränität" beitragen.[31] Möglich wäre letzteres aufgrund von „Datenspenden" sowie neuartiger Datenintermediäre, wie sie auch im Entwurf des Data Governance Act[32] beschrieben und Ziel der Europäischen Datenstrategie sind.

Neutrale Intermediäre als Chance für eine Kultur der Datennutzung

Wichtig wird dabei sein, die Neutralität dieser Intermediäre sicherzustellen – entweder durch die Bereitstellung von technischen Lösungen oder durch Plattformen, die keine eigenen Interessen verfolgen. Die wirtschaftliche Grundlage möglicher neuer Intermediäre ist noch nicht geklärt. Zwar genösse die öffentliche Hand als Betreiberin intermediärer Angebote stets einen Vertrauensvorschuss, doch sind gleichfalls privatwirtschaftlich betriebene Modelle denkbar. Zur wirtschaftlichen Grundlage von Datenintermediären hatte das Bundeswirtschaftsministerium im Sommer 2020 vorgeschlagen, dass Dienste, die die Verwaltung persönlicher Informationen anbieten, „kein wirtschaftliches Eigeninteresse an den im Auftrag der Endnutzer verwalteten Daten" haben dürften und zudem unabhängig von Unternehmen sein müssten, die ein solches Interesse haben[33]. Ein davon zu unterscheidendes wirtschaftliches Partizipieren am Bereitstellen der Plattform und Anbieten der Dienstleistung des Datenverwaltens müsste dagegen das neutrale Agieren der Plattform nicht behindern.

Die institutionelle Ausgestaltung solcher Intermediäre bedarf zukünftig besonderer Betrachtung. Im Sinne der Bekanntmachung des Bundesministeriums für Wirtschaft und Energie können auch solche „innovativen Datenökosysteme basierend auf der GAIA-X-Architektur" gefördert werden und dabei unterstützen, die Bereitstellung und Nutzung von Daten zu steigern.[34] Mit Blick auf die gerade genannten „Datenspenden" wäre empfehlenswert, frühzeitig die Überlegung anzustellen, wie eine entsprechende Einwilligung unter Beachtung der Voraussetzungen der DSGVO gestaltet werden müsste.[35] Für den wissenschaftlichen

Forschungsbereich privilegiert die DSGVO die Datenverarbeitung. So wurde im Bereich der Forschung für medizinische Forschungsfragestellungen bereits in der Vergangenheit eine Einwilligungserklärung zur Nachnutzung klinischer Daten erstellt.[36]

Insgesamt ist es also nach wie vor sehr empfehlenswert, technische und organisatorische Möglichkeiten in Form von PIMS oder persönlichen Datenräumen zu erforschen, um die persönliche Kontrolle über Daten zu stärken, die Nutzung für Forschungszwecke auszuweiten und gleichzeitig Bedenken auszuräumen.

1 In Nr. 435/April 2021 der Reihe Analysen & Argumente hat P. Kuzev bereits darauf hingewiesen, dass die DSGVO explizit auch die Verarbeitung von Daten zur Bekämpfung vorsehe (Erwägungsgrund 46).

2 Pressemitteilung der Datenschutzaufsichtsbehörden Baden-Württembergs, Bayerns, Hessens und des Saarlands zu Microsoft Office 365: Bewertung der Datenschutzkonferenz zu undifferenziert – Nachbesserungen gleichwohl geboten; abrufbar unter: www.lda.bayern.de/media/pm/20201002_office365.pdf (letzter Aufruf: 25.5.2021).

3 Gutachten der Datenethikkommission von 2019, S. 103; abrufbar unter: https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_DE.html?nn=11678504 (letzter Aufruf: 25.5.2021).

4 Beitrag des Beraters der EU-Kommission Paul Nemitz auf der Veranstaltung von Stiftung und Berufsverband der Datenschutzbeauftragten vom September 2020; Bericht abrufbar unter: www.datenschutz-notizen.de/diskussion-um-die-zukunft-der-datenschutzaufsicht-1827260/ (letzter Aufruf: 25.5.2021).

5 Datenschutz besser koordinieren und effektiver durchsetzen; Text bei der Europäischen Akademie für Informationsfreiheit und Datenschutz, abrufbar unter: www.eaid-berlin.de/datenschutz-besser-koordinieren-und-effektiver-durchsetzen (letzter Aufruf: 25.5.2021).

6 Siehe auch Gutachten der Datenethikkommission, S. 136 ff.

7 Betroffene gelten im Sinne der datenschutzrechtlichen Begriffsbestimmung als natürliche Personen, deren personenbezogene Daten verarbeitet werden.

8 Verantwortlicher im Sinne der Terminologie des Datenschutzrechts.

9 Siehe Stiftung Datenschutz, abrufbar unter: https://stiftungdatenschutz.org/themen/datenportabilitaet/ (letzter Aufruf: 25.5.2021). Die Stiftung Datenschutz verfolgt dieses Thema seit 2017 intensiv und lud im Herbst 2019 Akteurinnen und Akteure aus Politik, Aufsichtsbehörden, Wirtschaft, Wissenschaft und Gesellschaft zu mehreren Rundtischgesprächen ein, um ihre Erfahrungen zu teilen und um den aktuellen Stand zu diskutieren, siehe hierzu unter: https://stiftungdatenschutz.org/fileadmin/Redaktion/Datenportabilitaet/SDS_Datenportabilitaet-PolicyPaper2020-05-22_DE.pdf (letzter Aufruf: 25.5.2021).

10 Im Whitepaper von Facebook zur Datenportabilität wird Marc Zuckerberg zitiert (siehe S. 6, abrufbar unter: https://about.fb.com/wp-content/uploads/2020/02/data-portability-privacy-white-paper.pdf ; letzter Aufruf: 25.5.2021): Danach sollten Nutzer in die Lage versetzt werden, ihre Informationen direkt an einen Anbieter ihrer Wahl zu übertragen, vergleichbar mit dem Facebook-Login. Dies sei auch der Grund, warum sich Facebook am „Data Transfer Project" beteiligt. Gemäß diesem Whitepaper ist Aufgabe dieses Open-Source-Softwareprojekts, an dem u. a. auch Google, Microsoft, Twitter, Apple teilnehmen, gemeinsam wechselseitig kompatible Systeme zu entwickeln, die es Nutzern und Nutzerinnen erleichtern, ihre Daten problemlos zwischen Anbietern von Onlinediensten zu übertragen.

11 Siehe unter: https://www.dataportabilitycooperation.org/assets/Telecoms_Secured_Data_Hub.pdf (letzter Aufruf: 25.5.2021).

12 Siehe unter: https://www.anewgovernance.org/ (letzter Aufruf: 25.5.2021).

13 Diese Leitlinien wurden vom Europäischen Datenschutzausschuss bestätigt. Wie beim Europäischen Datenschutzausschuss (EDSA) handelte sich auch bei der Artikel-29-Datenschutzgruppe um eine unabhängige europäische Einrichtung, die zur einheitlichen Anwendung der Datenschutzvorschriften in der EU beiträgt sowie die Zusammenarbeit zwischen den EU-Datenschutzbehörden fördert und sich aus Vertreterinnen und Vertretern der nationalen Datenschutzbehörden und dem Europäischen Datenschutzbeauftragten zusammensetzt.

14 Siehe WP 242 Guidelines on the right to data portability vom 5.4.2017, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/wp/20170405_wp242_rev01.pdf (letzter Aufruf: 25.5.2021), S. 21.

15 Siehe WP 242, S. 3, 11, 21. Siehe bereits Benedikt, RDV 2017, S. 190; Jüllicher / Röttgen / v. Schönfeld, ZD 2016, S. 359, die ein aktives Tun als Voraussetzung ablehnen. Außerdem Herbst in: Kühling/Buchner, Art. 20 DSGVO Rn. 9 ff.

16 Siehe hierzu auch Datenethikkommission, S. 136 ff., abrufbar unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf;jsessionid=0DF3A869A43958956C9B8E5378E4AA8E.1_cid295?__blob=publicationFile&v=6 (letzter Aufruf: 25.5.2021).

17 Siehe Erwägungsgrund 55 des Entwurfs einer DSGVO (2012), Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) vom 25.1.2012, KOM (2012) 11 (abrufbar unter: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:de:PDF, letzter Aufruf: 25.5.2021).

18 Jüllicher / Röttgen / v. Schönfeld, ZD 2016, S. 360/362; Hennemann, Ping 01.17., S. 6; Strubel, ZD 8/2017, S. 359 mit dem Hinweis, dass ursprünglich angedacht war, das Recht auf Datenübertragbarkeit auf die Angebote Sozialer Medien zu begrenzen; Schätzle, Ping 02.16, S. 74 mit dem Hinweis auf die Kritik, dass es bei dem Recht auf Datenübertragbarkeit nicht um den Schutz der Privatsphäre gehe, sondern es sich vielmehr um ein wettbewerbspolitisches Instrument handele. Siehe außerdem Herbst in: Kühling / Buchner, Art. 20 DSGVO Rn. 4 ff.

19 Hennemann, Ping 01.17., S. 6 mit Verweis auf den wettbewerblichen Ansatz sowie auf die Aussage von Jan Albrecht (Berichterstatter des Europäischen Parlaments zur DSGVO), der in Artikel 20 einen Katalysator eines Wettbewerbs um datenschutzfreundliche Technologien sieht.

20 WP 242 Guidelines on the right to data portability vom 5.4.2017. S. 3, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/wp/20170405_wp242_rev01.pdf (letzter Aufruf: 25.5.2021).

21 Wobei der Begriff der Datensouveränität noch der Auslegung bedarf, siehe Projektgruppe „Datensouveränität", abrufbar unter: https://zevedi.de/aktivitaeten/projekte/ (letzter Aufruf: 25.5.2021), in der die Verfasserin dieses Textes Mitglied ist.

22 Siehe auch WP 242, S. 12/13, wo darauf verwiesen wird, dass ein bewährtes Verfahren für sämtliche Verantwortliche, die personenbezogene Daten erhalten oder übermitteln, darin bestehe, Tools einzusetzen, die den betroffenen Personen ermöglichen, diejenigen Daten, die sie erhalten und übermitteln möchten, auszuwählen und etwaige Daten anderer Personen auszuschließen. Auf diese Weise könnten die Risiken für Dritte, deren personenbezogene Daten möglicherweise mitübertragen werden könnten, weiter verringert werden. Darüber hinaus sollten die Verantwortlichen Einwilligungsmechanismen für andere beteiligte Personen einführen, um die Datenübertragung in den Fällen zu vereinfachen, in denen solche Dritte bereit sind, ihre Einwilligung zu erteilen, weil sie bspw. ihre Daten an einen anderen Verantwortlichen übertragen möchten.

23 Ebenso hat die Datenethikkommission eine Evaluierung dahingehend angeregt, wie eine zunehmende Stärkung der Marktmacht weniger Anbieter verhindert werden könne, sofern Art. 20 DSGVO nicht nur Anbieterwechsel erleichtern, sondern auch den Datenzugang für andere Anbieter verbessern soll. Siehe Datenethikkommission, S. 136 ff., abrufbar unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf;jsessionid=0DF3A869A43958956C9B8E5378E4AA8E.1_cid295?__blob=publicationFile&v=6 (letzter Aufruf: 25.5.2021) sowie unter https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission-kurzfassung.pdf?__blob=publicationFile&v=4, S. 14 (letzter Aufruf: 25.5.2021).

24 Siehe zum Begriff der „Digitalen Souveränität" als „Fähigkeit einer Entität, über die zukünftige Ausgestaltung festgestellter Abhängigkeiten in der Digitalisierung selbst entscheiden zu können und über die hierfür notwendigen Befugnisse zu verfügen" Steiner / Grzymek, Digitale Souveränität in der EU, abrufbar unter: https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/Digitale_Souveraenitaet_in_der_EU_Policy_Brief_BSt_EZ_European_Public_Goods_DE.pdf, S. 7 (letzter Aufruf: 25.5.2021).

25 Studie der Stiftung Datenschutz, „Neue Wege bei der Einwilligung", abrufbar unter: https://stiftungdatenschutz.org/themen/einwilligung-und-pims (letzter Aufruf: 25.5.2021).

26 Siehe Studie der Stiftung Datenschutz a. a. O.

27 Siehe unter: https://edps.europa.eu/data-protection/our-work/subjects/systeme-de-gestion-des-informations-personnelles_de (letzter Aufruf: 25.5.2021).

28 Eine solche Verwaltungsmöglichkeit von Daten hat die Stiftung Datenschutz ebenso in ihrer Studie untersucht. Ein Dienst hatte das Ziel, Nutzerinnen und Nutzer bei Ausübung ihrer Einwilligung automatisiert zu. Hierbei sollte die Zustimmung für unterschiedliche Datenverarbeitungsprozesse und Empfänger im Voraus erteilt und die persönlichen Daten dezentral bei der betroffenen Person gespeichert werden.

29 Siehe Studie der Stiftung Datenschutz a. a. O. sowie unter https://stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/PIMS-Abschluss-Studie-30032017/stiftungdatenschutz_Stellungnahme_Rechtliche_Aspekte_eines_Einwilligungsassistenten_Anhang_1_final.pdf (letzter Aufruf: 25.5.2021).

30 Siehe Studie von Conpolicy (2020): Innovatives Einwilligungsmanagement, abrufbar unter: https://www.conpolicy.de/referenz/innovatives-datenschutz-einwilligungsmanagement/ (letzter Aufruf: 25.5.2021).

31 Siehe zu den Begriffen der Digitalen Souveränität und Datensouveränität oben unter dem Punkt „Datenportabilität".

32 Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über europäische Daten-Governance (Daten-Governance-Gesetz) vom 25.11.2020, abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52020PC0767&from=EN (letzter Aufruf: 25.5.2021).

33 erster inoffizieller Entwurf zum TTDSG vom Juli 2020, abrufbar unter: https://cdn.netzpolitik.org/wp-upload/2020/08/20200731_RefE_TTDSG-clean.pdf (letzter Aufruf: 25.5.2021).

34 Siehe „Innovative und praxisnahe Anwendungen und Datenräume im digitalen Ökosystem GAIA-X", abrufbar unter: https://www.bmwi.de/Redaktion/DE/Downloads/F/foerderbekanntmachung-innovative-und-praxisnahe-anwendungen-und-datenraeume-im-digitalen-oekosystem-gaia-x.pdf?__blob=publicationFile&v=4 (letzter Aufruf: 25.5.2021).

35 Siehe insbesondere auch Erwägungsgründe 23 und 39 des Daten-Governance-Gesetzes.

36 Es haben sich bspw. alle Universitätsmedizinstandorte auf einen einheitlichen Mustertext geeinigt, zu welchem die Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder am 15. April 2020 ihr Einverständnis gegeben hat. Siehe hierzu unter: https://www.medizininformatik-initiative.de/de/mustertext-zur-patienteneinwilligung (letzter Aufruf: 25.5.2021).

Impressum

Die Autorin und der Autor

Prof. Dr. Anne Riechert ist Wissenschaftliche Leiterin der Stiftung Datenschutz. An der Frankfurt University of Applied Sciences ist sie seit 2009 als Professorin für Datenschutzrecht und Recht in der Informationsverarbeitung berufen. Sie ist außerdem Vorstandsmitglied des Netzwerks AI Frankfurt Rhein-Main e.V. und stellvertretende Leiterin des Zentrums verantwortungsbewusste Digitalisierung (zevedi.de).

Frederick Richter, LL. M. ist seit 2013 Vorstand der von der Bundesregierung gegründeten Stiftung Datenschutz. Zuvor arbeitete er als rechtspolitischer Berater im Bundestag und Datenschutzbeauftragter eines Wirtschaftsverbandes. Frederick Richter ist Mitglied der Fokusgruppe Datenschutz des Digital-Gipfels der Bundesregierung.

Konrad-Adenauer-Stiftung e. V.

Dr. Pencho Kuzev
Datenpolitik
Analyse und Beratung
T +49 30 / 26 996-324
pencho.kuzev@kas.de

Postanschrift: Konrad-Adenauer-Stiftung, 10907 Berlin

Herausgeberin: Konrad-Adenauer-Stiftung e. V. 2021, Berlin
Gestaltung & Satz: yellow too, Pasiek Horntrich GbR
Die Printausgabe wurde bei copy print Kopie & Druck GmbH, Berlin gedruckt.
Printed in Germany.
Gedruckt mit finanzieller Unterstützung der Bundesrepublik Deutschland.

ISBN 978-3-95721-931-2