Stellungnahme
in Form von Antworten zum Fragenkatalog

Öffentliche Anhörung des Ausschuss Digitale Agenda 24. Februar 2021 zu:

- „Datenstrategie der Bundesregierung“ – BT-Drs. 19/26450
- „Eckpunkte einer Datenstrategie der Bundesregierung“ – BT-Drs. 19/16075
- Antrag der Fraktion der FDP „Datenpolitik für Selbstbestimmung, Wettbewerb und Innovation“ – BT-Drs. 19/26538

Sachverständiger: Frederick Richter, LL.M.

VORBEMERKUNG

Die Datenstrategie der Bundesregierung adressiert wichtige Herausforderungen auf dem Weg zu besserer Datennutzung zum Wohl der Gesellschaft. Ein ausgeweitetes Nutzen von Daten als Schlüssel zum schnelleren Erreichen gesamtgesellschaftlicher Ziele ist legitimes Ziel der Datenpolitik.

Das Grundrecht auf Datenschutz und die EU-Datenschutzgrundverordnung werden zu Recht von der vorgelegten Datenstrategie als Fundament betrachtet, auf dem die Vorschläge aufsetzen.

Vordringlichstes Ziel muss Klarheit im Bereich der Anonymisierung sein.
Ohne klare Vorgaben zu einer hinreichenden Anonymisierung kann das Zeil der Daten-strategie eines ausgeweiteten Datenzugangs nicht erreicht werden. Öffentliche Maßgaben und Handlungs-anleitungen, entwickelt im Benehmen mit den unabhängigen Datenschutz-aufsichtsbehörden auf nationaler und europäischer Ebene könnten die bestehenden Rechtsunsicherheiten abbauen und die Bereitschaft zum freiwilligen Datenteilen erhöhen.

Der Ausbau von Maßnahmen zur Steigerung von Datenkompetenz und Datenbewusstsein ist Grundlage für einen bewussteren Umgang mit Daten, sowohl durch wirtschaftliche Akteure als auch durch die Nutzerinnen und Nutzer.

Wir begrüßen, dass sich die Bundesregierung gegen die Schaffung eines „Dateneigentum“ ausspricht. Ein derartiges Verfügungsrecht an Daten wäre mit dem europäischen Datenschutzrechtsregime nicht kompatibel. Auch würde ein solches Konstrukt weniger Probleme lösen als es schaffte.

Im Folgenden wird auf einzelne Fragen eingegangen. Aufgrund der Kurzfristigkeit konnte nicht auf alle Fragen tiefer eingegangen werden; nicht eigegangen werden konnte zudem auf Themenpunkte, die außerhalb des Fokus des Tätigkeitsfeldes der Stiftung Datenschutz liegen.

1. Allgemein

- **Wie bewerten Sie die grundsätzliche Zielrichtung der Datenstrategie mit Blick auf die vier zentralen Handlungsfelder?**

Die Datenstrategie adressiert eine der zentralen Herausforderungen dieser Zeit, nämlich die Unternutzung von Daten. Eine Hebung ungenutzter Potentiale von Daten zum allgemeinen Wohl bei gleichzeitiger Wahrung des datenbezogenen Grundrechtsschutzes ist übergeordnetes Ziel. Die Ausweitung einer grundrechtsschonenden Datennutzung ist sowohl geeignet, wirtschaftliches Wachstum zu fördern wie auch Ressourcenschonung und Gesundheit zu unterstützen. Das Spannungsfeld zwischen intensiverer und extensiverer Datennutzung einerseits und der Abwehr von Risiken für die Datensubjekts andererseits bedarf abgewogener regulatorischer Maßnahmen und hohem Datenbewusstsein. Von daher ist es richtig, dass die Bundesregierung nicht allein auf mehr Zugang und Nutzung von Daten abzielt, sondern die Kompetenz in Bezug auf Daten als gleichberechtigten weiteren zentralen Baustein danebenstellt. Die gewünschte neue Datenkultur sollte begriffen werden als konsequente Zusammenführung einer Datennutzungskultur mit einer Datenschutzkultur.

- **Wo sehen Sie welchen Änderungs- und/oder Ergänzungsbedarf? Findet die Datenstrategie einen angemessenen Ausgleich zwischen dem grundrechtlich garantierten Schutz vor allem personenbeziehbarer Daten und der Zugänglichmachung von Daten im Sinne des Gemeinwohls?**

Indem die Datenstrategie die Grundsätze des gegebenen Datenschutzrechts nicht in Frage stellt, respektiert sie klar das erreichte hohe Datenschutzniveau in der Europäischen Union. Auf dieser Basis dieser eindeutigen Ausgangslage lässt sich ein angemessener Ausgleich gut erzielen. Neue Regelungen zur Nutzung von Daten sollten gleichwohl keine Unsicherheiten für die Rechtspraxis auslösen. Rechtsunsicherheiten mögen nicht nur die mit der Strategie beabsichtigte Datennutzung schmälern; sie können auch zu Fehlern in der Rechtsanwendung und damit zu Risiken für Persönlichkeitsrechte führen.

- Welche Gründe sind aus Ihrer Sicht ursächlich dafür, dass bisher in Deutschland zu wenig Daten genutzt und geteilt werden?

Zentraler Grund für eine allgemeinwohlbezogen unbefriedigende Zugänglichmachung und Nutzung von Daten sind aus hiesiger Sicht Unsicherheiten bezüglich des rechtlichen Dürfens und Haftungsfragen.

Die Komplexität des Datenschutzrechts führt bei vielen Akteuren zu einer großen Zurückhaltung, wenn es darum geht, Daten der eigenen Organisation dem Wettbewerb, der Forschung oder der Allgemeinheit zur Verfügung zu stellen. Der verschärfte Sanktionsrahmen der DSGVO mag diese Zurückhaltung noch gesteigert haben. Bevor man – potentiell teure – rechtliche Fehler bei einer nicht gesetzlich geschuldeten Datenbereitstellung machen könnte, unterlässt man das Vorhaben oft lieber.

Weiterhin von Bedeutung sein dürfte das Fehlen von konkreten Anreizen zum Datenteilen bzw. die fehlende Wahrnehmung etwaig bestehender Anreize. Eine politisch erwünschte jedoch nur abstrakt beworbene „Förderung des allgemeinen Wohls" als solches kann in der Abwägung eines Unternehmens sehr leicht hinter Aspekte der Rechtskonformität zurückfallen. Im Fokus der Rechtsabteilung und der Leitung eines Unternehmens dürfte zunächst die angestrebte Rechtskonformität im Datenschutzbereich stehen, hinter der eine Datenteilungskultur heutzutage meist zurücktritt (soweit sie überhaupt besteht). In herkömmliche, in der Wirtschaft bereits verfolgte Nachhaltigkeitsstrategien hat die Datenteilung noch wenig Eingang gefunden. Berücksichtigt werden könnte das Allgemeinwohl als Datennutzungsziel konsequent in Rahmen einer „Corporate Digital Responsibilty", deren aussichtsreiche Bewerbung bei der Unternehmensdarstellung den benötigten Anreiz liefern könnte. Doch stehen derartige Programme noch vereinzelt und jeweils am Anfang.

- **Die in der Datenstrategie benannten Maßnahmen, um das Teilen nicht-personenbezogener Daten in der Wirtschaft zu forcieren, beschränken sich auf Standardsetzung und Prüfaufträge zu bspw. sektoralen Datenteilungspflicht oder einer möglichen weiteren Anpassung des Wettbewerbsrechts. Wird dies der zentralen staatlichen Aufgabe, öffentliche, digitale Infrastruktur bereitzustellen, gerecht?**

Ein Hauptgrund für Unsicherheiten beim Personenbezug und damit zugleich ein Hauptgrund für das häufige Unterlassen des Teilens von Daten sind fehlende Standards zum Anonymisieren. Die Setzung von Standards durch die öffentliche Hand oder zumindest die Förderung der Entstehung von Standards ist daher vordringliche staatliche Aufgabe. Inwieweit womöglich danach auch öffentliche Infrastruktur bereitzustellen wäre, kann diskutiert werden. In Betracht kämen dabei öffentlich entwickelte Instrumente zur Anonymisierung.

- **Halten Sie auch staatliche Förderungen für die Bereitstellung der Dateninfrastruktur bspw. in Form von Anschubfinanzierungen für den Aufbau von Datentreuhandstellen/Datenpooling-Stellen für zielführende Maßnahmen?**

Ja, soweit das Setzen von Standards allein deren Aufbau nicht bewirken kann.

- **Wie bewerten Sie, auch vor dem Hintergrund des Zeitpunkts der Vorlage der Datenstrategie, die Chancen, dass Teile der Datenstrategie - insofern sie nicht ohnehin bereits laufende Gesetzesvorhaben betreffen - noch in dieser Wahlperiode in konkrete gesetzgeberische Initiativen umgesetzt werden?**

Angesichts von noch acht verbleibenden Sitzungswochen in dieser Legislatur erscheinen die Chancen für erfolgreiche Abschlüsse gesetzgeberische Initiativen nicht groß. Von daher sollte parallel zu noch möglicher Gesetzgebung vor allem die Chance genutzt werden, diejenigen Maßnahmen der Datenstrategie umzusetzen, die auch ohne parlamentarisches Verfahren Wirkung entfalten können. Hier ist aus unserer Sicht vor allem zu nennen die Forschungsförderung für Anonymisierungsverfahren und die Erprobung von Innovationen in Reallaboren und untergesetzliche Maßnahmen zur Steigerung der Datenkompetenz.

- **Sehen Sie Widersprüche bezüglich der Datenstrategie und aktuellen Gesetzesvorhaben der Bundesregierung, etwa mit Blick auf das Bekenntnis für den Schutz personenbeziehbarer Daten?**

Laufende ebenso wie neue Gesetzgebungsvorhaben mit Bezug zu den Zielen der Datenstrategie sollten mit diesen eng abgestimmt (weiter)verfolgt werden, um keine Widersprüchlichkeiten aufkommen zu lassen. Eine grundrechtsschonende Ausgestaltung sollte zudem stets Leitschnur der Gesetzgebung sein.

- **Wie bewerten Sie die Anschlussfähigkeit der nationalen Datenstrategie hinsichtlich der europäischen Daten-Strategie und des Entwurfs eines "Data Governance Act" der EU-Kommission?**

Eine enge Abstimmung zwischen nationaler und europäischer Datenpolitik erscheint zwingend, nicht zuletzt mit Blick auf das vereinheitlichte Datenschutzrecht in der Europäischen Union. Wenn Standards zum Datenumgang gesetzt werden sollen, als bestenfalls internationale Orientierungspunkte, so kann dies nur im Verbund aussichtsreich erfolgen.

Diese notwendige Kongruenz sehen wir grundsätzlich als gegeben an. Die Zielvorstellungen der Digitalstrategie der EU-Kommission und der Datenstrategie der Bundesregierung gehen insbesondere bei der Datenteilung in die gleiche Richtung.

Zu begrüßen ist, dass sich das BMWi mit Blick auf die Schaffung eines Rechtsrahmens für EU-Datenräume für Akkreditierungen/Zertifizierungen von Treuhändern im Rahmen des Data Governance Acts einsetzen will.

- **Wie bewerten Sie die Datenstrategie der Bundesregierung hinsichtlich ihres vorgesehenen Monitorings?**

Wir begrüßen, dass eine Evaluation der Umsetzung der Datenstrategie zeitnah erfolgen soll.

Angesichts womöglich rascher Änderungen der Datennutzung in technischer/technologischer Hinsicht (z.B. neue Anonymisierungs- oder De-Anonymisierungsmöglichkeiten), in praktischer /wirtschaftlicher Hinsicht (neue Geschäftsmodelle; geändertes Nutzendenverhalten) und in rechtlicher Hinsicht (neue EU-Gesetzgebung) erscheint ein agiles Vorgehen beim Monitoring geboten.

Ebenso in den Blick genommen werden sollten zudem etwaige Wechselwirkungen und ggf. Überschneidungen mit weiteren einschlägigen Maßgaben und Beschlüssen und deren Umsetzungsstand. Zu denken ist hier an die datenpolitisch relevanten Punkte in folgenden teils bereits einige Zeit zurückliegenden Papieren:

- Umsetzungsstrategie der Bundesregierung „Digitalisierung gestalten“ (2020)
- Gutachten der Datenethikkommission (2019)
- Umsetzung der Digitalen Agenda der Bundesregierung (2017)
- Schlussbericht der Enquete-Kommission „Internet und digitale Gesellschaft“ (2013)

- **Welche konkreten Maßnahmen zur Unterstützung für Vereine und andere ehrenamtliche Strukturen (wie z.B. Hack-Spaces) und das digitale Ehrenamt allgemein sollten bei der Umsetzung der Datenstrategie realisiert werden?**
- **Gibt es spezifische datenpolitische Bedarfe von Zivilgesellschaft und Nichtregierungsorganisationen und sehen Sie diese in der Datenstrategie ausreichend berücksichtigt?**
- **Welche Maßnahmen zur Unterstützung gemeinwohlorientierter Datenprojekte sollten bei der Weiterentwicklung bzw. Umsetzung der Datenstrategie aufgenommen werden?**

In Bereich von Ehrenamt und bürgerschaftlichem Engagement besteht noch Potential zum Ausbau von Datenkompetenz und Datenschutzwissen. Wir begrüßen ausdrücklich das Ziel der Datenstrategie, die Kompetenz von zivilgesellschaftlichen Organisationen zum Umgang mit Daten zu stärken und sie beim sicheren und datenschutzkonformen Einsatz datenbasierter Prozesse unterstützen. Wir unterstützen dieses Ziel aktiv, indem wir in diesem Jahr unsere Aktivitäten zum Erklären von Datenschutzvorgaben für ehrenamtlich Engagierte und kleine Vereine ausbauen.

2. Dateninfrastruktur

- **Was muss mit Blick auf Daten- und IT-Sicherheit und auf die digitale Selbstbestimmung und Souveränität passieren? Wie können sichere und vertrauenswürdige Datenräume und Räume für Datenkooperationen geschaffen werden? In welchem Ausmaß kann GAIA-X einen Beitrag dazu leisten, die informationelle Selbstbestimmung und digitale Souveränität in Deutschland und Europa zu stärken? Welche Aspekte sind für die Etablierung eines europäischen Datenökosystems bei der aktuellen Konzeption des Projekts GAIA-X noch nicht gewürdigt oder berücksichtigt worden?**

Für den Erfolg von Initiativen wie GAIA-X erscheint aus Datenschutzsicht vor allem Vertrauen in deren DSGVO-Konformität bedeutsam. Beim Nachweis dessen kann die Zertifizierung nach Art. 42 DSGVO belastbare Unterstützung bieten. Ein Vorantreiben dieses wichtigen – aber bislang für die Praxis leider nicht zur Verfügung stehenden – Instruments wäre wünschenswert, z.B. durch öffentliche Förderung von Projekten wie AUDITOR (www.auditor-cert.de) oder Unterstützung und Beschleunigung der Anstrengungen der Deutschen Akkreditierungsstelle.

3. Datennutzung

- **Nicht aufgegriffen wurde in der Datenstrategie eine - ggfs. zunächst für bestimmte Sektoren ausgestaltete - Datenteilungspflicht. Wie sehen Sie Deutschland und Europa diesbezüglich aufgestellt und wo sehen Sie welchen regulativen Handlungsbedarf mit Blick auf die verschiedenen Akteurinnen und Akteure?**

Es ist grundsätzlich angemessen, zunächst auf anreizbezogene Ansätze zur Steigerung der Bereitschaft zum Datenteilen zu setzen und erst bei deren Scheitern über Zwangsmaßnahmen zu beraten. Auf dem derzeitigen Erkenntnisstand erscheint die Prüfung ausreichend, ob auf besonders datengetriebenen Märkten eine Verpflichtung zum Teilen von bestimmten Daten erforderlich sein kann. Allerdings sollte diese Prüfung ergebnisoffen sein.

Da mit Blick auf Marktmacht und deren möglichen Missbrauch vor allem wettbewerbs-bezogene Fragen betroffen sind, erscheint das Wettbewerbsrecht passender Ort für eine Datenzugangsregulierung. Die Novellierung des Gesetzes gegen Wettbewerbs-beschränkungen ist daher ein Schritt in die richtige Richtung.

- **Wie bewerten Sie die Option, Daten unter bestimmten Voraussetzungen zu vergesellschaften, also eine Art Datenteilungspflicht einzuführen?**

Bei Versagen anreizbezogener Lösungen können pflichtbezogene Lösungen diskutiert werden. Eine Vergesellschaftung von Daten im engeren Sinne kommt jedoch insofern nicht in Frage, als dass es kein Eigentum an Daten gibt. Es käme eher eine allgemeine Datennutzungserlaubnis in Betracht; eine solche könnte allein anonyme Daten umfassen.

- **Welchen flankierenden Regelungsbedarf sehen Sie im Hinblick auf eine etwaige Datenteilungspflicht im Bereich des Datenschutzes?**

Das Datenschutzrecht setzt einer Datenteilungspflicht eine Grenze, sobald die zu teilenden Daten Personenbezug oder Personenbeziehbarkeit aufweisen. Eine Datenteilung braucht bereits nach geltendem Recht eine Rechtsgrundlage gemäß Art. 6 Absatz 1 DSGVO.

- **Inwieweit sehen Sie im Datenschutzrecht im Hinblick auf die Erhebung und Verarbeitung personenbezogener Daten weiteren Regelungsbedarf?**

Die Verarbeitung personenbezogener Daten (die Erhebung ist bereits eine Verarbeitung) ist umfangreich reguliert. Defizite zeigen sich eher bei der tatsächlichen Datenkontrolle der betroffenen Personen. Diese haben zwar weitreichende Betroffenenrechte. Sie sind aber darauf verwiesen, diese selber auszuüben. Jede/r kann zwar von sämtlichen Unternehmen Auskunft über sie oder ihn betreffende Datenverarbeitung verlangen. Dies ist aber aufwendig und bisweilen abschreckend. Lösungen zur Behebung dieses Informationsdefizits mögen jedoch eher im technischen Bereich zu suchen sein und sodann gesetzlich unterstützt werden (siehe Antwort zu PIMS).

- **Wie könnten innovative Datenschutzeinwilligungsmanagements aussehen?**

Zur möglichen Gestaltung von Systemen zu einem innovativen Einwilligungsmanagement hat das vom BMJV geförderte Projekt der Organisation ConPolicy im Herbst vergangenen Jahres konkrete Vorschläge vorgelegt[1].

- **Sehen Sie die Notwendigkeit der Aufstockung des Personals der Datenschutzaufsichtsbehörden, die auch für die unabhängige Beratung von Bürgerinnen und Bürgern sowie Unternehmen zuständig sind?**

Ja.

- **Inwiefern ist eine Erweiterung des Datenschutzrahmens im Hinblick auf sogenannte Mixed Data Sets notwendig, die immer auch personenbezogene Daten beinhalten?**

Sobald auch personenbezogene Daten beinhaltet sind, gilt in Bezug auf diese das Datenschutzrecht mit all seinen Regelungen. Schwer vorstellbar ist daher eine Relativierung des Datenschutzrahmens bei gemischten Datensätzen, die das bisherige Schutzniveau absenkt.

- **Sowohl der Wert von Daten als auch die Kategorisierung der Datenart sind stark abhängig vom Verwendungskontext. So können scheinbare Maschinendaten je nach Verwendungszweck auch personenbezogene Daten sein. Inwiefern berücksichtigt die Datenstrategie diese Dynamik der Datenökonomie?**

Das Datenschutzrecht erlaubt keine privilegierende Sonderbehandlung von Maschinendaten, falls diese durch Kontextualisierung Personenbezug erhalten. Die Datenstrategie berücksichtigt diese – für die Praxis der Datenwirtschaft mitunter problematische – Konstellation, indem sie Vorschläge zum Instrument der Anonymisierung macht.

[1] Abschlussbericht Innovatives Datenschutz-Einwilligungsmanagement, abrufbar unter: www.conpolicy.de/referenz/innovatives-datenschutz-einwilligungsmanagement

- **Inwiefern bedarf es einer rechtlichen Grundsatzentscheidung in Bezug auf nicht-personenbezogene Daten? Wäre beispielsweise die Einführung einer Positivliste plastischer Regelbeispiele für nicht-personenbezogene Daten ratsam?**

Die Grundsatzentscheidung ist gefallen, indem nicht-personenbezogene Daten vom Anwendungsbereich des Datenschutzrechts ausgeschlossen wurden. Die DSGVO findet laut Art. 2 Abs. 1 i.V.m. Art. 4 Nr. 1 Anwendung auf personenbezogene Daten. Daraus lässt sich umgekehrt schließen, dass sie auf nicht-personenbezogene Daten eben keine Anwendung findet. Doch in der Tat besteht Klärungsbedarf. Denn die DSGVO regelt die Thematik nur in diesem juristischen „Umkehrschluss" und nicht ausdrücklich; lediglich in der Gesetzes-begründung (Erwägungsgrund 26) wird klargestellt, was anonyme Daten sind und dass die DSGVO für anonyme Daten nicht gilt. Zum Vorgang des Anonymisierens äußert sich das Gesetz nicht. Eine Definition kennt das EU-Datenschutzrecht leider nicht; sie findet sich allein im Datenschutzgesetz von Nordrhein-Westfalen (dort in § 3 Abs. 7).

- **Wie kann die Aufsichtsstruktur in Deutschland im Bereich Datenschutz optimiert werden, um die Komplexität und teilweise widersprüchliche Rechtsauslegung und Rechtsanwendung abzubauen, ohne das Datenschutzniveau abzusenken oder notwendige bereichsspezifische Regelungen zu beschränken?**

Zu dieser Frage hat die Stiftung Datenschutz im September 2020 eine Tagung durchgeführt, auf der das Für und Wider einer etwaigen Zentralisierung der Datenschutzaufsicht über den nicht-öffentlichen Bereich diskutiert wurde[2]. , über mögliche Folgen für die Praxis und über Chancen für Kompromisslösungen (Video-Mitschnitt unter https://sds-links.de/Aufsicht). Dabei wurde im Konsens zwischen allen Beteiligten deutlich, dass das Ziel aller Bemühungen nicht unbedingt eine Veränderung der Behördenstrukturen sein muss, wohl aber eine deutliche Verbesserung der Abstimmung.

Mehrere Kompromissvorschläge liegen vor: Eine Möglichkeit ist es, die Zuständigkeit des Bundesbeauftragten auf solche Unternehmen auszuweiten, die im Dax- oder MDax gelistet sind, sowie auf Unternehmen gleicher oder größerer Kapitalisierung, während die übrigen Unternehmen weiterhin unter Landesaufsicht bleiben. Ein anderer Vorschlag zieht eine Parallele zur Rundfunkaufsicht und orientiert sich an deren Struktur. Dies umfasste eine Vereinheitlichung des Landesrechts, die Errichtung einer gemeinsamen Geschäftsstelle und eine Delegation gewisser Entscheidungskompetenzen an diese Einrichtung. Analog zu den im Rundfunkrecht bestehenden Kommissionen könnten im Datenschutz die von allen Aufsichtsbehörden gemeinsam gebildeten Arbeitskreise zur Festlegung von für alle Bundesländer verbindlichen Rechtsauslegungen ermächtigt werden. Ein Vorschlag des ehemaligen Bundesbeauftragten Peter Schaar plädiert zwar dafür, die Datenschutzaufsicht weiterhin in der Fläche zu belassen, sieht aber zwingendes Kohärenzverfahren für die Konferenz der deutschen Datenschutzbehörden vor. Es ist dem Vorbild des von der DSGVO für die europäische Ebene der Aufsicht vorgeschriebenen Kohärenzverfahrens nachgebildet.

[2] Bericht und Aufzeichnung der Konferenz „Die Zukunft der Datenschutzaufsicht – föderal oder dezentral" abrufbar unter: www.stiftungdatenschutz.org/aufsicht-live

Als Schritt in Richtung verbesserter Effektivität fungierte ein Bund-Länder-Staatsvertrag, der die Koordinationsmechanismen der DSGVO auf den Bundesstaat Deutschland überträgt. In streitigen Fragen würde dann die DSK verbindliche Mehrheitsentscheidungen treffen – unter Umständen auch gegen das Votum der federführenden Landesbehörde. Ein solches Modell ist der deutschen Aufsicht nicht völlig fremd, denn das BDSG sieht es bereits für die nationale Vorbereitung von Beschlüssen des Europäischen Datenschutzausschusses vor.

- **Wie kann die Nachnutzung, insbesondere bei Forschungsdaten, zukünftig besser gewährleistet werden? Was sind derzeit die größten Herausforderungen im Bereich der rechtssicheren Nachnutzung von Daten?**

Jedenfalls bei personenbezogenen Daten wird für die Nutzung zu einem anderen Verarbeitungszweck als den ursprünglichen u.U. eine neue/eigene Rechtsgrundlage notwendig sein. Wenn für die Nachnutzung/Weiterverarbeitung die ursprüngliche Rechtsgrundlage genutzt werden soll, muss der Verantwortliche prüfen, ob die Verarbeitung zu dem anderen Zweck mit dem ursprünglichen Zweck vereinbar ist; erleichternd wirkt dabei z.B. eine Pseudonymisierung.

- **Vielfach besteht Unsicherheit, wann eine hinreichende Anonymisierung vorliegt. Ist eine (unwiderrufliche) Anonymisierung Ihrer Ansicht nach überhaupt darstellbar? Welche Anonymisierungsverfahren und -methoden finden derzeit hauptsächlich Anwendung, welche gilt es speziell zu fördern? An welchen Stellen ist Vorsicht geboten hinsichtlich der Nutzung von Anonymisierung und Pseudonymisierung von Daten und welchen Regelungsbedarf gibt es gegebenenfalls?**

Orientierungspunkte für eine hinreichende Anonymisierung fehlen. Noch gibt es keinerlei Normen oder Standards für den relevanten Vorgang des Anonymisierens. Wie eine hinreichend belastbare Anonymisierung erreicht werden kann, dazu gibt es bislang keine offiziellen Maßgaben, keine Kurzpapiere, Entschließungen, Orientierungshilfen oder andere Anwendungshinweise – weder von der Konferenz der deutschen Datenschutzaufsichts-behörden, noch vom EU-Datenschutzausschuss. Auch DSGVO-Verhaltensregeln, wie sie zur Pseudonymisierung immerhin im Entwurf vorliegen, gibt es nicht. Nur der BDI und der BITKOM haben im vergangenen Jahr erste privatwirtschaftliche Vorstöße zu Handlungsanleitungen angestoßen.
Dies bewirkt Unsicherheiten in Bezug auf das Datenteilen und ganz allgemein in Bezug auf das Nutzen anonymer Daten. Denn wenn mangels Regelung die zu erfüllenden Voraussetzungen für eine belastbare und rechtssichere Anonymisierung unklar sind, kann dies im Effekt dazu führen, dass Daten nicht genutzt werden, obwohl von ihnen mangels Personenbezug eigentlich gar kein Risiko für Rechte und Freiheiten natürlicher Personen mehr ausgehen kann.

Dieser Mangel an Orientierung sollte behoben werden. Neben öffentlichen Leitlinien sind alternativ Verhaltensregeln nach Art. 40 DSGVO denkbar, wie sie auch zur – praktisch nicht weniger bedeutsamen – Pseudonymisierung angestrebt werden.

Die beim IT-Gipfel der Bundesregierung gebildete Fokusgruppe Datenschutz, in der auch die Stiftung Datenschutz mitwirkt, hat zum Digitalgipfel 2019 einen entsprechenden Entwurf vorgelegt[3].
Ebenso wie der Pseudonymisierung kommt der Anonymisierung eine Ermöglichungsfunktion zu. Sie kann den von der Datenstrategie zu fördernden Datenzugang dort ermöglichen, wo sie bei bestehendem Personenbezug datenschutzrechtlich schwer möglich wäre.

- **Der Datenraum der öffentlichen Verwaltung soll der Datenstrategie zufolge neben optimierter Datenhaltung und Datenpflege auch zur Datensparsamkeit beitragen. Wie bewerten Sie das Ziel der Datensparsamkeit im Kontext der Verarbeitung nicht-personenbezogener Daten?**

Das alte BDSG verpflichtete in § 3a zur „Datenvermeidung und Datensparsamkeit", also dazu, die Datenverarbeitung „an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen."
Nach der Verpflichtung aus der DSGVO zur „Datenminimierung" (Art. 5 Abs. 1 lit. c) muss die Verarbeitung personenbezogener Daten „dem Zweck angemessen sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein".

Für personenbezogene Daten kommt es nach dem neuen europäischen Datenschutzrecht nicht mehr auf ein „so wenig wie möglich" an, sondern allein auf Angemessenheit und Notwendigkeit. Wenn die Verarbeitung vieler Daten für den verfolgten legitimen Zweck erforderlich ist, dann verlangt das Datenschutzrecht auch keine Verringerung der Datenmenge.

Bei nicht-personenbezogenen Daten gilt das Datenschutzrecht nicht. Daher gibt es für diese Daten – auch in Datenräumen der öffentlichen Verwaltung – keine Vorgaben zu Sparsamkeit.

- **Die Datenstrategie erwähnt das mitunter lebensrettende Potenzial von Daten im Bereich des Gesundheitswesens. Sind aus Ihrer Sicht personenbezogene Gesundheitsdaten mit Blick auf den intersektoralen Austausch, aber auch den teilweise in höchstem Maße sensiblen personenbeziehbaren Informationen besonderen Regularien zu unterstellen, insofern nicht ohnehin schon besondere Regeln für sie gelten?**

Es gelten bereits besondere Regeln, nämlich Art. 9 DSGVO und § 22 BDSG.

- **Ab 2023 sollen auf Grundlage einer informierten Einwilligung auch Daten aus der elektronischen Gesundheitsakte zu bestimmten Forschungszwecken freigegeben werden können.**

[3] Entwurf für einen Code of Conduct zum Einsatz DS-GVO konformer Pseudonymisierung; abrufbar unter: www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2019/p9-code-of-conduct.pdf?__blob=publicationFile&v=2

Wie beurteilen Sie die Bereitschaft zur Freigabe individueller Daten zu Forschungszwecken allgemein und konkret in diesem Bereich? Wie lässt sich die Bereitschaft zur Freigabe von Daten zu Forschungszwecken erhöhen? Welche Rolle spielen Datenschutz und Datensicherheit? Wie müssen Prozesse gestaltet sein, die zu einer tatsächlichen Informiertheit derjenigen führen, die über die Freigabe ihrer Daten entscheiden?

Bei Gesundheitsdaten ist die Bereitschaft zur „Datenspende“ einer Umfage des IT-Verbandes BITKOM hoch. Fast 90 % der Menschen in Deutschland seien der Befragung zufolge bereit, ihre Daten unter bestimmten Voraussetzungen nicht nur öffentlichen Forschungsinstituten, sondern auch privatwirtschaftlich getragener Forschung zur Verfügung zu stellen[4].

Weiteres Indiz für eine Offenheit gegenüber einer zielgerichteten und zweckgebundenen Freigabe von Gesundheitsdaten ist die Nutzung der Datenspende-App des Robert-Koch-Instituts, für deren Unterstützung mehr als 500.000 Nutzer ihr Fitnessarmband oder ihre Smartwatch mit der App verknüpften und ihre Zustimmung zur wissenschaftlichen Datenauswertung gaben.

Dem Aspekt der Informiertheit muss bei allem großes Augenmerk gegeben werden, denn gerade bei sensiblen Daten sollten nur bewusste Entscheidungen durch die Datensubjekte getroffen werden.

- **Vertrauenswürdige Intermediäre wie Datentreuhänder können einen wichtigen Beitrag zum Datenzugang und -austausch leisten. Bisher haben sich kaum Datentreuhänder in unserem Datensystem etabliert. Was halten Sie dafür für ursächlich? Welche Akteure kommen für Sie als neutrale Intermediäre in Frage?**

Verantwortlich für die bisher fehlende Etablierung waren bislang Unklarheiten über Funktion, Struktur und rechtlichen Rahmen einer Datentreuhand[5]. Der mit der Datenstrategie unternommene Vorstoß zur Klärung ist zu begrüßen – ebenso das in ihr gemachte Versprechen, „keine neue Bürokratie“ schaffen zu wollen und den Datenaustausch nicht erschweren. Diese Vorgabe lässt sich in gewisser Weise als bewusste Kontrastierung zu den parallel entstandenen Maßgaben im Brüsseler Data Governance Act zum freiwilligen Datenteilen verstehen, nämlich den Regelungen zu einem “Datenaltruismus”, im Rahmen dessen die Datennutzung für Gemeinwohlzwecke gefördert werden soll. Dazu werden viele neue Verfahrensschritte und sogar neue Institutionen vorgeschlagen und die Umstände insgesamt recht komplex gestaltet. So sollen die Mitgliedstaaten jeweils ein “Register anerkannter datenaltruistischer Organisationen” einrichten.

---

[4] Große Offenheit für Spende von Patientendaten; BITKOM-Umfrage vom Juli 2020, Zusammenfassung abrufbar unter: www.bitkom.org/Presse/Presseinformation/Grosse-Offenheit-fuer-Spende-von-Patientendaten

[5] siehe Bestandsaufnahme „Themenpapier Datentreuhandmodelle“ April 2020, abrufbar unter: https://pure.mpg.de/rest/items/item_3222478_1/component/file_3222479/content

Diese datenteilenden Organisationen müssen wiederum genaue Aufzeichnungen über alle datenverarbeitenden Personen, Zeitpunkte und Zwecke der Datenverarbeitung führen. Sie sollen Tätigkeitsberichte erstellen müssen und neben den datenschutzrechtlichen Informationspflichten weitere Informationspflichten erhalten. All dies klingt nicht unbürokratisch und könnte das Vorankommen des Datenteilungssektors dämpfen.

- **Welche Datentreuhandmodelle gelten in den unterschiedlichen Sektoren derzeit als erfolgversprechend? Welche Datentreuhandmodelle kommen insbesondere auch auf der Ebene von Einzelpersonen beziehungsweise im Bereich B2C in Betracht?**

Neben der von der Datenstrategie hauptsächlich favorisierten Funktion der Datenzugangsförderung sind sehr unterschiedliche Funktionen von Datentreuhandeinrichtungen denkbar, die sektorspezifisch variierbar sein können:

- Stärkung individueller Kontrolle über Datenflüsse
- Förderung der Teilhabe der Datensubjekte an wirtschaftlicher Verwertung von Daten
- Förderung von Datenteilung und Verfügbarmachung von Daten zur Förderung von Innovation und Wettbewerb
- Bereitstellung qualitativ hochwertiger Daten für Wissenschaft und Forschung
- Einschränkung der marktbeherrschenden Stellung großer Plattformbetreiber
- Förderung vertrauenswürdiger europäischer Plattformangebote
- Bildung eines Vertrauensankers und

Im B2C-Bereich bietet ein Unternehmen aus Bochum bereits Dienstleistungen als Datentreuhand an (www.datatrustee.org/datentreuhand).

- **Wie kann ein Datenmanagementsystem für Verbraucherinnen und Verbraucher (PIMS) in der Praxis aussehen?**

Den Ansatz der Personal Information Management Systems/Services (PIMS) hat die Stiftung Datenschutz 2016/2017 in einem Projekt untersucht[6]. Solche Softwarelösungen speichern und/oder verwalten persönliche Daten entsprechend den Vorgaben der Nutzerinnen und Nutzer. Teils wird auch ein Einwilligungsmanagement bezweckt oder eine ausgeweitete Datenkontrolle bzw. -Übersicht, mittels „Privacy Dashboards“ und ähnlichen Werkzeugen. Die meist plattformunabhängigen Dienste bieten ein breites Funktionsspektrum - von simplen Kalenderlösungen bis hin zur Vermarktung nutzerbezogener Daten. In der Regel stehen die Anwendungen als kostenlose Add-ons oder Apps zur Verfügung.

[6] Studie: "Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen", abrufbar unter: https://stiftungdatenschutz.org/themen/pims-studie

Die Idee hinter solchen Ansätzen ist, dass es dem Nutzer möglich sein soll zu entscheiden, wann, an wen, zu welchem Zweck, in welchem Umfang und für wie lange er seine Daten übermittelt. Gleichzeitig soll damit die Nutzung der Daten nachverfolgt und ggf. widerrufen werden können.
Eine allgemeine Definition von PIMS existiert bisher 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 „technologiegestützte Anwendung zum Aufbau von Ökosystemen, mit deren Hilfe Personen in die Lage versetzt werden, die Sammlung und Verarbeitung, die Verbreitung sowie den Austausch ihrer persönlichen Daten besser zu überblicken und zu steuern“[7].

- **Das in der Datenschutzgrundverordnung explizit angelegte Recht auf Datenportabilität (Artikel 20 DSGVO) wird durch die Datenstrategie nicht explizit aufgegriffen. Halten Sie es für geboten dieses Instrument für eine souveräne Datennutzung weiter auszugestalten?**

Zum Art. 20 DSGVO legte die Stiftung Datenschutz in 2017 eine Studie vor[8] und die weitere Entwicklung des Rechts auf Datenübertragung im Herbst 2019 unter Mitwirkung von Akteuren aus Politik, Aufsichtsbehörden, Wirtschaft, Wissenschaft und Gesellschaft in drei Workshops diskutiert.

In der Praxis gibt es noch immer wenig Erfahrungswerte zum Umgang mit dem Recht auf Datenübertragbarkeit. Insgesamt besteht jedoch ein großer Bedarf an einer umfassenden Analyse dahingehend, wie sich das Portabilitätsrecht auf Datenökonomie und Gesellschaft auswirkt und welchen technischen Herausforderungen begegnet werden muss. So befassen sich aktuell verschiedene Initiativen mit diesem Thema, wie etwa das „Data Transfer Project“ großer amerikanischer Digitalkonzerne, die „Data Portability Cooperation“ unterschiedlicher Telekommunikationsanbieter oder die Initiative „New Governance“ mit dem Fokus auf einen branchen- und sektorübergreifenden Datentransfer. Aus datenschutzrechtlicher Sicht muss bei sämtlichen Aktivitäten die Stärkung des Kontrollrechts der Betroffenen im Mittelpunkt stehen, so dass neue Geschäftsmodelle dieses Kontrollrecht nicht aushebeln.

Eine weitere Ausgestaltung des Rechts auf Datenportabilität und Datenportierung sollte abzielen auf die Herstellung von Interoperabilität zwischen Diensten.

Auch Datentreuhandlösungen könnten bei der Operationalisierung des Datenübertragungs-rechts hilfreich sein.

---

[7] Arbeitspapier der Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft im Rahmen des Digital-Gipfels 2020, S. 8; abrufbar unter: www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2020/p9-datenmanagement-und-datentreuhandsysteme.pdf?__blob=publicationFile&v=2

[8] Wege zur praktischen Umsetzung des Rechts auf Datenübertragbarkeit; abrufbar unter: https://stiftungdatenschutz.org/themen/datenportabilitaet

- **Die digitale Datennutzung wird vielfach über Einwilligung in Allgemeine Geschäftsbedingungen (AGBs) geregelt. Halten Sie die Zertifizierung von AGBs für geboten?**

Zivilrechtlich meinen „Allgemeine Geschäftsbedingungen" für eine Vielzahl von Verträgen vorformulierte Vertragsbedingungen, die typischerweise vorgegebene Regelungen zu Zahlungsarten, Versandbedingungen u.ä. enthalten. Im Gegensatz dazu sollen Unternehmen in einer Datenschutzerklärung ausschließlich darüber informieren, wie sie mit personenbezogenen Daten von Kundinnen und Kunden umgeht. Oft werden beide Dokumente vermischt, was hinsichtlich der vom Datenschutzrecht geforderten Transparenz und Klarheit problematisch sein kann. Eine in AGB gleichsam versteckte Einwilligung genügt den Anforderungen der DSGVO nicht.

Eine generelle (Vorab-)Prüfung von AGB und/oder Datenschutzerklärungen, z.B. durch Datenschutzaufsichtsbehörden dürfte bereits wegen der Anzahl jener nicht möglich sein. Interessant könnten dagegen technische Lösungen sein, die den Inhalt von Datenschutzerklärungen analysieren und für die Nutzenden bewerten[9].

- **Welchen rechtlichen Handlungsbedarf sehen Sie beim Thema Delegierbarkeit von datenschutzrechtlichen Einwilligungen oder zumindest typisierter Entscheidungen im Kontext informationeller Selbstbestimmung? Wie lässt sich eine Delegierbarkeit konkret gesetzlich umsetzen?"**

Eine Möglichkeit zum Delegieren von Einwilligungsentscheidungen könnte die Verbraucherschaft im digitalen Alltagsumfeld erheblich entlasten. Wenn digitale Werkzeuge im Dienst und Auftrag der sie einsetzenden Person nach deren festgelegten Präferenzen Zustimmungen zur Datenverwendungen geben oder verweigern, so würde dies der „Einwilligungsmüdigkeit", ausgelöst durch ständige Anfragen, entgegenwirken.

Datenschutzrechtlich ist die Umsetzung solcher digitaler Einwilligungsassistenten problematisch, da Einwilligungen nach der DSGVO für den konkreten Einzelfall bewusst/informiert abgegeben werden müssen und eine lediglich generalisierende Vorfestlegung mit konkreter Ausübung durch Dritte/Software nicht vorgesehen ist. Hierzu müsste eine Klarstellung im Gesetz erfolgen, z.B. durch eine Ergänzung in einem Art. 7 Abs. 2 Satz 3 DSGVO-neu:

> „Die Einwilligung kann auch durch elektronische Mittel erfolgen, soweit sichergestellt ist und nachgewiesen werden kann, dass die Bedingungen, unter denen die Einwilligung erfolgt, den zuvor getroffenen Festlegungen der betroffenen Person entsprechen".

[9] z.B. das Projekt DATENSCHUTZscanners (PGuard), Informationen unter: https://datenschutz-scanner.de/detail/news/forschungsprojekt-veroeffentlicht-gemeinsamen-abschlussbericht

- **Welchen rechtlichen Handlungsbedarf sehen Sie bei den Vorschriften zur AGB-Kontrolle in Bezug auf die Überprüfbarkeit datenschutzrechtlicher Einwilligungen in Nutzungsbedingungen, insbesondere betreffend die Bewertung von Umfang, Zweck und Dauer eingeholter datenschutzrechtlicher Einwilligungserklärungen?**

Es ist zulässig, Einwilligungserklärungen in Allgemeine Geschäftsbedingungen zu integrieren. Werden aber datenschutzbezogene Bedingungen in AGB geregelt, müssen diese „gemischten Geschäftsbedingungen" sowohl den Anforderungen des Zivilrechts als auch denen des Datenschutzrechts genügen, d.h. BGB und DSGVO. Es gilt damit bereits ein doppelt strenger Maßstab für die Gültigkeit von „Daten-AGB".

Das Landgericht München beispielsweise erklärte 2019 eine Einwilligung in AGB als unzureichend, die nicht hervorgehoben dargestellt war und konkrete Datenkategorien nicht nannte. Das Kammergericht (Berlin) unterwarf in 2018 die Datenschutzrichtlinie von Apple der zivilrechtlichen AGB-Kontrolle, weil es davon ausgeht, dass Apple den Eindruck erwecke, es würde sich nicht bloß um Informationen zum Datenschutz handeln, sondern um verbindliche vertragliche Regelungen.

4. Datenkompetenz

- **Die Relevanz von Datenkompetenz in der Wirtschaft nimmt stetig zu. Wie bewerten Sie die Vielfalt der derzeitigen Angebote und Förderungen zur Vermittlung für Datenkompetenz im Bereich mittelständiger Unternehmen? Wie, bzw. mit welchen Mitteln kann die Datenkompetenz in der Gesellschaft, insb. bei KMU erhöht werden? Inwieweit sind die hierfür in der Datenstrategie vorgeschlagenen Maßnahmen geeignet?**

Datenkompetenz im Mittelstand ist unerlässlich. Die Stiftung Datenschutz trägt hier seit einigen Jahren nach ihren (vom Bund noch auszubauenden) Kapazitäten zur Erklärung von Datenschutzanforderungen bei, z.B. mit der Broschüre „Datenschutz im Betrieb"[10].
Eine Vielfalt von Angeboten schadet dann nicht, wenn keine inhaltlichen Widersprüche auftreten.
Die BMWi-Initiativen Mittelstand-Digital und Go-Data erscheinen als sehr gut nutzbare Instrumente zur Vermittlung von Datenkompetenz in der Wirtschaft.

- **Wie viele Fachkräfte im Bereich Datenverarbeitung wird Deutschland in den nächsten Jahren benötigen? Und wie kann Deutschland diesen Bedarf decken?**

Der Fachkräftebedarf in der datenbasierten Wirtschaft wird weiter steigen.

[10] https://stiftungdatenschutz.org/themen/datenschutz-im-betrieb

- **Wie bewerten Sie die Maßnahmen zur Datenkompetenzvermittlung im zivilgesellschaftlichen Bereich mit Blick auf die aktuellen Herausforderungen aufgrund der COVID-19-Pandemie, der beispielsweise Vereine begegnen müssen. Wie steht es dabei insbesondere um die Kompetenz im Umgang mit der Datenschutzgrundverordnung?**

Der Vermittlungsbedarf ist pandemiebedingt sprunghaft angestiegen, da viele Prozesse aus dem Stand heraus digitalisiert werden mussten – wobei der Ausbau der Datenkompetenz und besonders der Datenschutzkompetenz nicht Schritt halten konnten.

Daher startet die Stiftung Datenschutz in diesen Monaten in Kooperation mit der Deutschen Stiftung für Engagement und Ehrenamt das Aktionsprogramm „Datenschutz im Ehrenamt“.

- **Wie sehen Sie zivilgesellschaftliche Organisationen bisher aufgestellt?**

Oftmals haben sich gerade kleinere Verein bisher nicht in dem Maße mit Fragen von Datenschutz und Datensicherheit befasst, wie es die pandemiebedingte Digitalisierung nun von ihnen verlangt. Als Beispiel ist zu nennen der datenschutzgerechte Einsatz von Videokonferenzdiensten, z.B. zur Durchführung von Beratungsdienstleistungen oder von Vereinssitzungen.

- **Wie bewerten sie die Datenkompetenz in Deutschland im Vergleich zu anderen europäischen Staaten?**

Ohne hierzu konkrete Zahlen nennen zu können, liegt Deutschland schätzungsweise im Vergleich zu anderen Staaten im oberen Feld. Besonders Datenschutzfragen haben in Deutschland traditionell einen hohen Stellenwert.