Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Deutscher Bundestag
Ausschuss Digitale Agenda

Ausschussdrucksache
19(23)111

Bonn, den 22.02.2021

Stellungnahme

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zur öffentlichen Anhörung des Ausschusses Digitale Agenda

am 24. Februar 2021

zu den Eckpunkten einer Datenstrategie der Bundesregierung

I. Zusammenfassung:

1. Die Eckpunkte für eine Datenstrategie der Bundesregierung zielen ebenso wie die EU-Datenstrategie primär auf die Schaffung einer digitalen Datenwirtschaft. Nach der Datenschutz-Grundverordnung (DSGVO) und dem Ausbleiben einer datenschutzfreundlichen ePrivacy-Verordnung bedeuten diese Planungen durchaus einen grundlegenden Perspektivwechsel der EU. Die jetzt geplante, weitere Kommerzialisierung des Umganges auch mit personenbezogenen Daten und das Anwachsen des Datenhandels schaffen erhebliche Risiken für die Datenschutzrechte der Bürger.
2. Die Erwartungen der Bürgerinnen und Bürger an den Schutz ihrer Privatheit und den Datenschutz in der Digitalisierung sind dagegen gleichbleibend hoch. Wirkungsvolle Datenschutzkonzepte und funktionsfähige Datenschutzbehörden sorgen mit für das notwendige Vertrauen in den digitalen Wandel. Ausreichende Befugnisse und die angemessene Ausstattung der Behörden auch und gerade auf Länderebene bilden hierfür eine Grundlage.
3. Die mit der Datenstrategie verbundenen Veränderungen sowohl für die Rechte der Bürgerinnen und Bürger als auch für die Demokratie bedürfen einer aktiven Gestaltung und Weiterentwicklung des bestehenden Datenschutzsystems. Für die Weiterentwicklung hat insbesondere die Datenethikkommission weiterreichende Vorschläge unterbreitet, die leider kaum Eingang in die Datenstrategie gefunden haben.
4. Informationsfreiheit, Open Data, Open Source und Informationssicherheit zählen zu übergreifenden, auch und gerade die Interessen der Bürgerinnen und Bürger in der Digitalisierung schützenden Zielen und Konzepten und ermöglichen ihre Teilhabe an diesem Prozess.

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

5. Ich begrüße das Bekenntnis der Datenstrategie zu einer verantwortungsvollen Datennutzung. Konkrete Maßnahmen fehlen allerdings überwiegend und müssen folgen. Konzepte der Datentreuhänderschaft bieten Chancen und Risiken. In Bezug auf die Verwaltung von personenbeziehbaren Big Data-Seen bergen sie massive Risiken und erfordern eine zusätzliche datenschützende Einhegung.
6. Statt des verdinglichenden Datenbegriffes im Sinne eines „Dateneigentums“ sollte eine Datenwirtschaft den Leitbegriff der Information und damit auch die Wissensperspektive betonen. Damit werden die gesellschaftlichen Herausforderungen nicht allein für den Datenschutz, sondern auch mit Blick auf Daten als öffentliches Gut und die Potentiale von Open Source, Open Data und Stärkung von Demokratiestrukturen besser sichtbar.
7. Im Rahmen der Datenstrategie können Fortschritte und Weiterentwicklungen bei Anonymisierungs- und Pseudonymisierungskonzepten, bei datenschutzbezogenen Datentreuhandmodellen, bei den sog. *Privacy (oder Personal) Information Management-Systemen* (PIMS) sowie dezentrale Datenhaltung und Datenportabilität neu entstehende Gefährdungen der Persönlichkeitsrechte zum Teil einhegen oder kompensieren helfen. Doch es kommt auf die konkreten Konzepte an, die mit den genannten Schlagworten verbunden werden.
8. Der Verweis auf das „Unberührtbleiben“ der DSGVO wird angesichts der Dimension der geplanten Handelbarkeit von Daten kaum genügen und verschleiert die tatsächlichen Auswirkungen auf Datenschutz und informationelle Selbstbestimmung. Zum einen müssen mögliche Konflikte mit Datenschutzbestimmungen offen benannt und gelöst werden. Zum anderen bedarf es angesichts der dynamischen Rechtsentwicklung sowohl auf europäischer als auch nationaler Ebene auch der Weiterentwicklung des Privatheitsschutzes, um das Schutzniveau zu erhalten.

II. Allgemeines

1. BfDI begrüßt die Datenstrategie

Angesicht der Fülle von den Datenschutz berührenden Einzelmaßnahmen der vorliegenden Datenstrategie der Bundesregierung können hier nur einige grundsätzliche Anmerkungen erfolgen. Insbesondere werden die den Datenschutz besonders berührenden Vorschläge des 2. Kapitels im Vordergrund stehen.

Ich begrüße grundsätzlich die Vorlage einer Datenstrategie durch die Bundesregierung. Sie kann angesichts der vielen, bei einer Datenökonomie sich aufdrängenden Fragen einen wichtigen politischen Orientierungspunkt bieten. Denn die Bürgerinnen und Bürger haben einen Anspruch darauf zu verstehen, in welcher Weise ihre Interessen und Rechte durch das Handeln der Bundesregierung im digitalen Wandel berührt werden. Längst hat die Digitalisierung neben den rein technischen Veränderungen auch einen tiefgreifenden gesellschaftlichen Wandel ausgelöst. Sie schafft neben zahlreichen Chancen auch grundlegende Risiken und ist daher selbstverständlich auch mit Ängsten verbunden. Gerade im Umgang mit den

persönlichen Daten der Bürgerinnen und Bürger bei Unternehmen und Verwaltung wird dies besonders deutlich.

Es ist deshalb grundsätzlich auch zu begrüßen, dass die Datenstrategie mehrfach klare Bekenntnisse zum bestehenden, auch europäischen Datenschutzstandard enthält und im Gefolge der Datenstrategie die Absicht geäußert wird, das gegenwärtige Datenschutzniveau zu wahren. Zutreffend wird auch betont, dass dafür Datenschutzprinzipien von Beginn bei der Entwicklung und Produktion sowie auf Infrastrukturebene Berücksichtigung finden müssen (mit den Prinzipien Privacy by Design und Privacy by Default). Positiv hervorzuheben ist auch die geplante Forschungsunterstützung im Bereich der Anonymisierungstechnologien.

Der Wert des Bekenntnisses der Datenstrategie zur ePrivacy-Verordnung wird sich allerdings noch erweisen müssen. Denn der deutschen Ratspräsidentschaft ist es in sechs Monaten nicht gelungen, die Vorlage mit den von ihr geforderten Verbesserungen des Schutzes der Online-Kommunikation voranzubringen. Stattdessen droht nach gegenwärtigem Verhandlungsstand die Wiedereinführung der Vorratsdatenspeicherung, die zulässige Weiterverarbeitung von Metadaten der Kommunikation unterhalb des DSGVO-Schutzniveaus sowie insgesamt die fehlenden Rückgriffsmöglichkeit auf schützende Bestimmungen der DSGVO.

Entgegen so manchen Äußerungen auch in der gegenwärtigen Corona-Pandemie bildet ein effektiver Datenschutz die Grundlage für die weitere Digitalisierung. Denn er sorgt letztlich für das notwendige Vertrauen in die Nutzbarkeit neuer Angebote und Dienstleistungen und damit die dringend benötigte Akzeptanz der Bürgerinnen und Bürger in eine Entwicklung, die weiterhin bei vielen mit Besorgnissen und Ängsten verbunden ist. Aufgrund der mit der DSGVO europaweit harmonisierten Voraussetzungen der Datenverarbeitung leistet der Datenschutz bereits einen Beitrag zum „free flow of personal data“ – die DSGVO bekennt sich schließlich in ihrem allerersten Satz (Art. 1 Abs. 1) ausdrücklich dazu. Er steht auch der kommenden Datenwirtschaft nicht entgegen, sondern erfordert als modernes Element unseres Rechtsstaates und der Grundrechtsordnung entsprechende Vorkehrungen zum Schutz der Rechte der Bürgerinnen und Bürger und der Demokratie in der Digitalisierung.

Der Datenschutz kann die an ihn gestellten hohen Erwartungen allerdings nur erfüllen, wenn er in Grundkonzeption, rechtlicher Ausgestaltung und tatsächlicher Ausstattung mit den gegenwärtigen dynamischen IT-Entwicklungen Schritt halten kann.

In dieser Hinsicht fallen bei der vorliegenden Stellungnahme zwei Punkte besonders auf:

Zum einen werden datenschutzrechtliche Fragen (insbesondere im 2. Kapitel) primär als mögliche Hindernisse für angestrebte Datennutzungen dargestellt und behandelt. Die darauf aufbauenden Maßnahmen werfen dementsprechend Fragen auf und überzeugen nicht durchgehend.

Zum anderen fehlt es insgesamt an konkreten Maßnahmen für Verbesserungen des Datenschutzes, wie sie etwa im Rahmen der Datenschutzethikkommission speziell mit Blick auf

die Datenökonomie, aber zu relevanten Einzelfragen auch in einer Vielzahl von Stellungnahmen der Datenschutzkonferenz und in den Tätigkeitsberichten des BfDI vorgeschlagen wurden.

2. Mehr Transparenz zum Regelungskontext der Datenstrategie erforderlich

Erschwert wird die Bewertung der vorliegenden Datenstrategie dadurch, dass die Bundesregierung keine übergreifende Einordnung zum politischen Gesamtkontext vorlegt. Hier wäre eine deutlich verbesserte Transparenz wünschenswert bzw. die Offenlegung der Dachstrategie geboten. Erst in der Zusammenschau der verschiedenen (zum Teil wohl auch vorab abgestimmten) komplexen Maßnahmen auf europäischer als auch nationaler Ebene wird die eingeschlagene Richtung deutlich und damit auch eine fundierte Kritik möglich.

Denn der gesetzliche regulatorische Rahmen auch für die vorliegende Datenstrategie wird im Wesentlichen aus Brüssel kommen. Jetzt wäre die Zeit, auch auf nationaler Ebene darüber breiter zu diskutieren und entsprechende Vorschläge einzubringen.

Die zu Beginn letzten Jahres veröffentlichte, primär wirtschaftspolitisch ausgerichtete Mitteilung zur EU-Datenstrategie (COM(2020) 66 final) zielt in einem Paket mit weiteren Maßnahmen auf die Stärkung der Digitalisierung der EU-Mitgliedstaaten, insbesondere im internationalen Wettbewerb etwa mit den USA und China. (Dazu hat u.a. der Europäische Datenschutzbeauftragte umfänglich Stellung genommen, vgl. Stellungnahme 3/2020 des EDSB, abrufbar unter https://edps.europa.eu/sites/edp/files/publication/20-06-16_opinion_data_strategy_de.pdf).). Inzwischen hat die EU-Kommission mit der Vorlage erster Entwürfe etwas mehr Klarheit geschaffen. Mit dem Data-Governance-Act, dem Digital Service Act sowie dem Digital Markets Act zeigen sich Umrisse einer Datenmarktpolitik, die auch Folgen für das Datenschutzgefüge in der EU nach sich zieht. Für das Verständnis der Datenstrategie der Bundesregierung von besonderer Bedeutung ist der Regelungsrahmen des Data-Governance-Act (deutsch: Daten-Governance-Gesetz, vgl. COM(2020) 767, abrufbar unter https://ec.europa.eu/commission/presscorner/detail/de/QANDA_20_2103), der zurzeit besonders viele Fragen aufwirft. Der Europäische Datenschutzausschuss als Zusammenschluss der Datenschutzaufsichtsbehörden der Mitgliedstaaten wird in Kürze dazu eine umfängliche Stellungnahme vorlegen. Weitgehend unbekannt ist, dass die Europäische Kommission zum 3. Quartal diesen Jahres noch einen sog. „Data Act“ vorstellen will, der vermutlich erst die entscheidenden Vorgaben und Umsetzungspflichten im Hinblick u. a. auch auf den Data-Governance-Act enthalten wird (so womöglich im Hinblick auf Datenportabilität, eine mögliche Datenteilungspflicht oder weitere Vorgaben zu den sog. Datenintermediären).

Schließlich wird auch die Verzahnung mit der KI-Strategie und darauf beruhenden Maßnahmen zu wenig deutlich. Denn immerhin steht im Mittelpunkt der Datenstrategie die Förderung sowohl von Big Data als auch die verstärkte Entwicklung und der Einsatzes von Künstlicher Intelligenz. Gerade die Konzepte von Big Data und KI werfen aber mit Blick auf die

Datenschutzprinzipien zahlreiche Fragen auf. Aus datenschutzrechtlicher Sicht werden erst in der Zusammenschau dieser beiden Verarbeitungskonzepte die damit verbundenen Risiken für Privatheit und Datenschutz angemessen bewertbar.

3. Informationen (und Wissen) statt Daten als Leitbegriffe im Blick halten

Datenstrategien setzen beim Datenbegriff an. Weil Daten vergegenständlicht in IT-Anlagen gespeichert und verarbeitet werden, besteht hier eine erste Ebene der Regelungsmöglichkeit (wie im Datenschutz), und es entsteht der Eindruck eines (dinglichen) Gegenstandes. Dabei sind Informationen die eigentliche Leitkategorie, nicht Daten. Daten sind die auf einem Datenträger festgehaltenen Zeichen, die als Informationsgrundlagen dienen (syntaktische Ebene). Als bloße Zeichen weisen sie für sich auch keinen Personenbezug auf. Informationen hingegen betreffen den Sinn, der aus Daten eben erst erzeugt werden muss, je nach bestimmten Kontexten, in denen aus Informationen dann auch Wissen entsteht (semantische Ebene). Auch der grundrechtliche Datenschutz kann genauer als ein Teil des grundrechtlichen Informationsschutzes verstanden werden.

Vor diesem Hintergrund ist es zunächst zu begrüßen, dass die Datenstrategie, wenn auch ohne nähere Erläuterungen einem „Dateneigentum“ eine Absage erteilt. Dateneigentum wäre die weitest gehende Umsetzung eines Konzeptes von Daten als privatwirtschaftliches Handelsgut. Doch solche dinglichen Rechte etwa an den Daten selbst (also auf der syntaktischen Ebene) würden im Falle des Personenbezuges in jedem Falle mit dem im grundrechtlichen Persönlichkeitsrecht verankerten Datenschutzrecht der Betroffenen kollidieren. Und mittelbar wären immer auch die aus den Daten entwickelbaren Informationen mitbetroffen.

Aus der Perspektive des Urheberrechts etwa würde durch Dateneigentum mittelbar stets der Grundsatz der Gemeinfreiheit von Informationen beeinträchtigt. Diese Perspektive der Gemeinfreiheit verweist auf den gänzlich anderen Regelungsansatz von Daten als einem öffentlichen Gut oder der Datenallmende. Unter diesem Ansatz werden gemeinwohlorientierte Projekte, etwa unter kommunaler Hoheit wie etwa bei Smart Cities-Projekten, verfolgt. Aufgrund der von den Interessen der Bürgerinnen und Bürger ausgehenden Planungsziele können rein gewerbliche Datensammlungen oft vermieden, Datenschutz, Partizipation der Betroffenen und Open Source hingegen in den Mittelpunkt gerückt werden.

Auch wenn die Datenstrategie kein Dateneigentum im engeren Sinne verfolgt: mit Begriffen wie Datennutzung, Datenteilen, Datentausch, Dateninhaber oder gemeinsame Datennutzung schafft die Datenstrategie (und mit ihr die EU-Rechtsakte) ein Vokabular, was den Eindruck beliebiger Handelbarkeit von Informationen und Daten noch verstärkt.

Die Datenstrategie enthält zudem einen Prüfauftrag für eine sog. Datenteilungspflicht, welche womöglich auch über den angekündigten EU-Data Act realisiert werden könnte. Aus der Datenschutzperspektive ist aber schon der Begriff des Datenteilens schwierig, wenn und soweit es sich um personenbeziehbare Informationen handelt. Denn der Datenschutz dient

gerade dem Ziel, eine Weitergabe dieser Informationen zu begrenzen bzw. die Mitsprache der Betroffenen zu sichern und an klare Bedingungen zu knüpfen. Eine grundrechtskonforme datenschutzrechtliche Ausgestaltung muss also Grundlage für die Ermöglichung solchen Umgangs mit Informationen und Daten sein.

Die in der Datenstrategie betonte Idee der Schaffung neuer Datenräume wirft aus datenschutzrechtlicher Perspektive Fragen auf. Insbesondere kann die damit einhergehende Suggestion eines praktisch ungehinderten Datenflusses auch personenbezogener Daten innerhalb eines neu geschaffenen Datenraumes nicht geteilt werden. Zentral dagegen steht hier das Zweckbindungsprinzip als schlechthin konstitutive Grundregel des Datenschutzes. Was aus datenökonomischer Sicht als vermeintlich datenflusshinderliches Datensilo eingestuft wird, kann aus datenschutzrechtlicher Perspektive genau zum Schutz der Informationen und Daten der von Verarbeitungen betroffenen Bürgerinnen und Bürger angezeigt und grundrechtlich geboten sein. Sollen also die Daten weiterfließen, bedarf es entsprechender Rechtsgrundlagen sowie weiterer Voraussetzungen wie etwa der Transparenz für die davon Betroffenen.

4. Nicht-personenbezogene Daten und Repersonalisierbarkeit

Mit Blick auf nicht-personenbezogene Datensätze mögen die verschiedenen Ansätze zur Schaffung von Datennutzungsrechten vertretbar erscheinen, weil dann der Anwendungsbereich der Datenschutzgesetze grundsätzlich nicht eröffnet wäre. Die Datenstrategie ebenso wie der übergeordnete Gesetzentwurf der EU-KOM zum DGA betrifft allerdings in wesentlichen Teilen auch den Umgang mit personenbezogenen Daten, vermeidet also gerade eine saubere Trennung der unterschiedlichen Regelungsebenen und trägt somit zur Verwirrung bei. Hintergrund dürfte die komplexe Realität der Big Data-Verarbeitung sein. Häufig wird es sich bei den entsprechenden Massendaten um sog. Mixed data sets handeln, bei denen in Teilen doch personenbeziehbare Daten enthalten sind. In diesem Fall sind die Datenschutzbestimmungen anwendbar. Umso bedeutsamer sind daher technische Verfahren zur De-Personalisierung bzw. zur Verhinderung der De-Anonymisierbarkeit entsprechender Datensätze. Die Stärkung der Forschung in diesem Bereich ist daher grundsätzlich zu begrüßen.

Abzulehnen ist hingegen die gesetzliche Gleichsetzung von Anonymisierung und Pseudonymisierung, wie dies auch im aktuell vorliegenden Entwurf des EU-Daten-Governance-Gesetzes in Bezug auf die Wiederverwendung von amtlichen Daten zu auch kommerziellen Zwecken geschieht. Die Regelung unterstellt in unzutreffender Weise die Möglichkeit beliebiger Weitergabe öffentlicher Datenbestände bei bloßer Pseudonymisierung, obwohl es aus datenschutzrechtlicher Perspektive keinen Zweifel geben kann, dass eine Pseudonymisierung nicht zu einer Aufhebung des Personenbezugs führt (vgl. EG 26, Art. 4 Nr. 5 der DSGVO).

Kritisch sehen wir, dass die Datenstrategie letztlich keine Antwort auf die grundlegende Frage gibt, wie die Trennung von Gesetzesregelungen zu personenbezogenen Daten und

nicht-personenbezogenen Daten in einer Digitalwirtschaft des Austausches von Daten und gemischten Datensätzen aufrechterhalten werden kann. Zunehmende Risiken der Re-Identifizierung legen nach unserer Auffassung eher die Erstreckung weiterer gesetzlicher Datenschutzvorkehrungen zum Schutz der Bürgerinnen und Bürger auch auf den Umgang mit nicht-personenbezogenen Daten nahe.

III. Zum I. Kapitel „Das Fundament: Dateninfrastrukturen leistungsfähig und nachhaltig ausgestalten“

Auf Infrastrukturebene sind die Ziele von Datenschutz und Datensicherheit als auch die Betonung der Ermöglichung dezentraler Strukturen, etwa im Rahmen von Gaia-X, besonders zu begrüßen. Präventiver Datenschutz kann nur gelingen, wenn er Berücksichtigung bereits bei der Konzeption, Planung und Produktion von Infrastrukturen und Verfahren findet. Privacy by Design verwirklicht demnach Datenschutzprinzipien oder Elemente davon zum frühestmöglichen Zeitpunkt.

Die Datenschutzkonferenz hat kürzlich in ihrem Beschluss zur Datensouveränität die besondere Bedeutung auch von Open Source für die Wahrnehmung datenschutzrechtlicher Verantwortung im Bereich der öffentlichen Verwaltung hervorgehoben.

Dezentral stattfindende Datenverarbeitungen vor Ort also wie z.B. im Smartphone, am Smart Meter Gateway selbst oder in der Onboard-Unit eines Fahrzeuges, können Möglichkeiten der Verfügbarkeit und der Ausgestaltung der Datenhoheit der von den Verarbeitungen betroffenen Bürgerinnen und Bürger sicherstellen.

Für ein Projekt wie Gaia-X begrüßen wir die Ausrichtung auf open source und die damit verbundene Überprüfbarkeit bzw. Nachvollziehbarkeit der eingesetzten Software, mit der auch Sicherheitsvorgaben des Datenschutzes erfüllt werden.

Beim Quantencomputing bedarf es zusätzlich einer Maßnahme zur Forschung zu den Auswirkungen auf den Datenschutz. Speziell zu den Folgen für Verschlüsselungsstandards bzw. den Entschlüsselungspotentialen des Quantencomputing sollten die Wissensgrundlagen dafür gefördert werden, dass Verschlüsselung weiter entwickelt werden kann und sicher bleibt.

IV. Zum II. Kapitel „Innovative und verantwortungsvolle Datennutzungen steigern“

Das 2. Kapitel der Datenstrategie berührt die Aufgabenbereiche des BfDI wie auch den meiner Kolleginnen und Kollegen in den Ländern am meisten. Allein das Kapitel 2.1 enthält 26 Forderungspunkte. Viele der genannten Punkte befinden sich bereits in Umsetzung.

Wir begrüßen, dass die Strategie die Ergebnisse insbesondere der Datenethikkommission (DEK) berücksichtigen will, die viele konkrete Vorschläge für den Erhalt von Privatheit in der Datenökonomie enthält. Gleichwohl haben die allerwenigsten Vorschläge Aufnahme in den Maßnahmenkatalog der Datenstrategie gefunden, was wir bedauern.

1. Datenschutzaufsicht

Die Struktur der Datenschutzaufsicht folgt der vom Grundgesetz vorgegebenen föderalen Struktur. Die Rechtsordnung selbst setzt hier entsprechende Grenzen der Zentralisierung. Die Aufsichtsbehörden praktizieren ihre Zusammenarbeit seit Jahrzehnten routiniert und vertrauensvoll. Die Kooperation ist im Rahmen der Umsetzung der DSGVO zuletzt deutlich vertieft worden. Gleichwohl wird die Datenschutzkonferenz selbst weitere Verbesserungsvorschläge vorlegen. Im Vordergrund steht dabei die Forderung nach Verstärkung und höherer Verbindlichkeit der Abstimmung zwischen den Behörden. Ich habe in diesem Zusammenhang die Schaffung eines ständigen Sekretariats der Datenschutzkonferenz angeregt, um die Zusammenarbeit weiter zu professionalisieren. Im Rahmen der in der Datenstrategie angesprochenen, laufenden Evaluation des Bundesdatenschutzgesetzes werden die Datenschutzbehörden beteiligt. Wir halten die Evaluierung des Bundesdatenschutzgesetzes für einen wichtigen Anlass und werden diesen Prozess mit eigenen Vorschlägen unterstützen. In einzelnen Bereichen wie etwa dem Gesundheitssektor bestehen durchaus komplexe Regelungslagen. Überwiegend hat dies mit föderalen Regelungsstrukturen zu tun.

Auch auf europäischer Ebene muss geprüft werden, auf welche Weise die Zusammenarbeit der Aufsichtsbehörden im Europäischen Datenschutzausschuss (EDSA) weiter effektiviert werden kann. Vor allem das sog. One-Stop-Shop-Verfahren funktioniert bislang nicht zufriedenstellend. Es ist daher zu überlegen, ob wichtige Fälle direkt dem EDSA zur Entscheidung zugeteilt werden. Auf einer gesonderten Arbeitsebene sollten diese priorisierten wichtigen Fälle vom EDSA selbst und schnell auf Basis eines europäischen Verfahrensrechts geklärt werden.

2. Federführende Datenschutzaufsicht

Kritisiert hatte ich im zurückliegenden Jahr bereits im Rahmen des Infektionsschutzgesetzes die Regelung des § 287a SGB-V, soweit damit die Koordinierung der Behörden der Länder und des Bundes erreicht werden soll. Der Bezug in der Norm auf Art 56, 60 DSGVO ist in der Praxis letztlich nicht umsetzbar. Das Mehr an Vereinheitlichung und ausreichende Ressourcen bei der Aufsicht bezüglich des Umganges mit Forschungsdaten könnten insoweit besser durch eine Koordination durch den BfDI erreicht werden.

Generell gilt, dass die Verarbeitung zu Forschungszwecken im Datenschutz seit jeher eine erhebliche Privilegierung erfährt. Die Zulässigkeit weiterer Forschungsklauseln sowie die erweiterte Verknüpfbarkeit von Forschungsdaten können nur im Kontext konkreter Gesetzgebungsvorhaben bewertet werden.

3. Anonymisierung

Ich begrüße die geplante Unterstützung der Forschung im Bereich Anonymisierung. Wie oben gezeigt, hat die erfolgreiche Anonymisierung von Big Data-Datenbeständen überragende Bedeutung für die weitere rechtliche Behandlung und auch scheinbar nicht-personenbezogene Datenbestände können durch Datenteilung und Datentausch stets der De-Anonymisierung unterfallen. Immerhin soll nun ein Forschungsnetzwerk angestoßen werden. Für die Rechte der Bürgerinnen und Bürger bieten effektive Anonymisierungen maximalen Schutz. Ich bedauere, dass die weitergehenden Vorschläge der Datenethikkommission nicht aufgegriffen wurden. Insbesondere wird ein Verbot der aktiven De-Anonymisierung von Datenbeständen nicht aufgegriffen, obwohl es etwa im Rahmen der jüngsten kalifornischen Datenschutzgesetzgebung Berücksichtigung gefunden hat. Zudem fehlen Maßnahmen zur Förderung der dringenden Standardisierung von Anonymisierungs- als auch Pseudonymisierungsverfahren. Forschung auch im Bereich sog. synthetischer Daten verdient ebenfalls weitere Prüfung.

4. Daten-Governance-Gesetz und Innovationsausschuss

Im Hinblick auf den Daten-Governance-Act (DGA) kritisiere ich die Darstellung dieser Vorhaben in der Datenstrategie unter der Rubrik nicht personenbezogene Daten. Das entspricht inhaltlich nicht der aktuell diskutierten gesetzlichen Vorlage aus Brüssel.

Es wird in der Datenstrategie leider nicht ansatzweise erläutert, wie diese Vorhaben konkret aus Sicht der Bundesregierung gestaltet werden sollten und wie der DGA mit der eigenen Datenstrategie verflochten ist. Hier wäre mehr Transparenz wünschenswert. Im Einzelnen ergeben sich folgende Problembereiche

a. Pauschale Erstreckung von Open Data auf personenbezogene Daten?

Ich unterstütze im Rahmen seiner Aufgabenerfüllung der Förderung der Informationsfreiheit die proaktive Bereitstellung öffentlicher, mit öffentlichen Steuermitteln generierten Informationen und Daten. Der aktuelle Entwurf des Daten-Governance-Act (DGA-E) geht allerdings, entgegen der bestehenden europäischen und bundesdeutschen Rechtslage, von einer zukünftig geltenden allgemeinen Wiederverwendbarkeit von in hoheitlicher Hand befindlichen amtlichen Informations- und Datenbeständen auf Antrag auch kommerzieller

Stellen aus und erfasst ausdrücklich ohne nähere Einschränkung auch personenbezogene Daten.

Damit würden beispielsweise selbst personenbezogene Sozial- und Gesundheitsdaten ebenso wie Registerdaten für allgemeine kommerzielle Datenauswertungen verfügbar. Zwar verneint der Gesetzentwurf die Schaffung einer entsprechend bindenden Rechtsgrundlage für die Bereitstellung der Daten, andererseits enthält er (vgl. etwa Art. 5 DGA-E) entsprechend interpretierbare, ambivalent formulierte Passagen. Zudem verweist die EU-Kommission auf die mögliche Schaffung entsprechender Rechtsgrundlagen etwa im Rahmen des geplanten EU-Data-Act oder auch durch die Mitgliedstaaten selbst. Der BfDI hielte eine derartige pauschale Entwicklung angesichts der damit verbundenen Eingriffe in die Rechte der Bürgerinnen und Bürger für nicht vertretbar. Insbesondere sind die entsprechenden amtlichen Datenbestände aufgrund gesetzlicher Vorgaben allein zu staatlichen Zwecken erhoben und verarbeitet worden. Sie können nicht beliebig an private Dritte, auch nicht auf dem Wege allein der Pseudonymisierung, zu kommerziellen Verwertungszwecken weitergegeben werden.

b. Datentreuhänderschaft

In das in der Datenstrategie mehrfach in Bezug genommene Konzept der Datentreuhänderschaft werden große Hoffnungen gesetzt. Auch die Datenethikkommission hat dazu Aussagen getroffen, allerdings ausschließlich auf ein bestimmtes, allein auf die bessere Wahrung und Unterstützung der Datenschutzrechte von Bürgerinnen und Bürgern ausgerichtetes Konzept. Danach liegt das Potential der Datentreuhänderschaft in einer Befähigung der Einzelnen zur besseren Ausübung ihrer Datenschutzrechte. Allerdings muss stets auch die Gefahr vermeintlicher Interessenwalter bedacht werden, die am Ende nur ihren Eigeninteressen nachkommen. Der rechtliche Rahmen für Datentreuhänder muss aus datenschutzrechtlicher Sicht so ausgestaltet werden, dass Interessenkonflikte der Datentreuhänder ausgeschlossen werden.

Ich habe mich u.a. mit dem Konzept der Datentreuhänder in Zusammenhang mit Privacy (oder Personal) Information Management Systems (PIMS) beschäftigt. Bei PIMS handelt es sich um digitale Dienstleistungen, die zum Ziel haben, den Betroffenen Kontrolle über ihre personenbezogenen Daten zu ermöglichen und sie von Entscheidungen zu entlasten, die sie überfordern.

Datentreuhand-Modelle im Rahmen der PIMS würden eine beauftragte und vordefinierte Fremdverwaltung der Daten der Nutzenden ermöglichen. Im Interesse der Rechtssicherheit wäre es wünschenswert, wenn die Aktivitäten im Rahmen von PIMS rechtlich klar umrissen wären. Aus datenschutzrechtlicher Sicht muss dabei stets die Frage im Auge behalten werden, inwiefern der nationale Gesetzgeber angesichts der Vorgaben des Europäischen Datenschutzrechts über Regelungsspielräume bei den individuellen Datenschutzrechten und de-

ren Delegation verfügt. Dies hängt auch davon ab, wie das jeweilige PIMS genau ausgestaltet ist. PIMS müssen jedenfalls eindeutig den Interessen der betroffenen Personen dienen und dürfen nicht an der Nutzung der Daten verdienen. Diese Forderung wurde durch den BfDI auch in das Gutachten der Datenethikkommission (DEK) eingebracht.

Der Entwurf des Daten-Governance-Act enthält eine erste Regelung (vgl. 3. Kapitel des DGA-E) der Datentreuhänderschaft unter dem Begriff der Dienste für die gemeinsame Datennutzung bzw. der Datenmittlerschaft. Dabei wird ein Rahmen für einige wenige abstrakt umschriebene Modelle (B2B, B2C, Datengenossenschaften) geschaffen. Zwar wird die Neutralität des Datenmittlers geregelt, aber es fehlen jegliche konkrete Regelungen für das Modell der datenschutzrechtlichen Treuhänderschaft. Zudem wird eine völlig neue Aufsichtsstruktur geschaffen. Dabei wird es sich bei den genannten Datenmittlern in aller Regel aus Datenschutzsicht um Datendrehscheiben für einen massenhaften Datenumschlag mit hohem Risiko für die Rechte der betroffenen Bürgerinnen und Bürger handeln. Zahlreiche konkrete gesetzliche Anforderungen an derartige Datenmittler wären im Einklang mit den Datenschutzprinzipien zu formulieren und aufgrund der Datenschutzrelevanz sollten die Datenschutzaufsichtsbehörden bei der Beaufsichtigung ein vorrangige Rolle spielen.

Mit Datenmittlern wäre im Kontext des Internet der Dinge etwa vorstellbar, dass die von Messgeräten wie Schrittzähler, Pulszähler usw. anfallenden Daten nicht direkt von Unternehmen wie Google Fitbit an Versicherungsunternehmen weitergegeben würden, sondern stattdessen über den die Akzeptanz sichernden Umweg eines entsprechenden Datenmittlers. Ob überhaupt und unter welchen Bedingungen diese Entwicklung gestaltet werden sollte, sollte offengelegt und transparent diskutiert werden.

Im Bereich der Wirtschaft werden Datentreuhandmodelle sowohl im B2B als auch im B2C-Bereich diskutiert. Im B2B-Bereich sollen durch Datentreuhänder gegenseitige oder auch einseitige Datennutzungsrechte zwischen Unternehmen eingeräumt werden. Mögliche Anwendungsgebiete sind der Zugriff auf Gerätedaten durch Hersteller und Nutzer in der Produktion, aber auch die Bereitstellung von Kundendaten an einen Dritten. Im B2B-Bereich ist immer zu prüfen, ob personenbezogene Daten betroffen sind. Dies kann bspw. auch bei Gerätedaten der Fall sein, wenn diese Rückschlüsse auf den bedienenden Mitarbeiter ermöglichen. Deshalb kommt der Weiterentwicklung auch des Beschäftigtendatenschutzes in der Datenökonomie eine wichtige Rolle zu. Sobald personenbezogene Daten betroffen sind, sind bei der Ausgestaltung eines Datentreuhandmodells die datenschutzrechtlichen Vorschriften einzuhalten. Sollen beispielsweise Kundendaten nur anonymisiert zur Verfügung gestellt werden, so ist u. a. genauestens zu prüfen, ob das Anonymisierungsverfahren wirklich zu anonymen oder nur zu pseudonymen Daten führt.

Im B2C-Bereich werden ebenfalls viele Datentreuhandmodelle diskutiert. Hierdurch sollen die Nutzer auch die Möglichkeit haben, „an der Wertschöpfung“ aus ihren Daten zu profitieren. Dieses Konzept hat Parallelen zur Diskussion um das „Dateneigentum“. Das Konzept des Dateneigentums wird vom BfDI und der Datenethikkommission abgelehnt. Solche Da-

tentreuhandmodelle im B2C-Bereich sind aus datenschutzrechtlicher Sicht jedenfalls kritisch zu hinterfragen und dürfen niemals das immateriell ausgerichtete Datenschutzrecht ersetzen, sondern können immer nur zusätzliche Mechanismen bereitstellen, um die Souveränität des Einzelnen zu stärken. Die Datenschutzkonferenz hat hierzu in ihrer „Göttinger Erklärung zum Wert des Datenschutzes in der digitalen Gesellschaft“ zentrale Aussagen getroffen.

Eine Vermischung von Datentreuhändern i. S. d. PIMS mit dem Wertschöpfungsansatz im B2C-Bereich sollte aus Datenschutzsicht nicht erfolgen. Hier sind Interessenkonflikte, die es auszuschließen gilt, vorprogrammiert.

c. Datenaltruismus

Nach dem DGA-E müssen die Mitgliedstaaten die Registrierung und eine gesonderte Aufsichtsstruktur für sog. datenaltruistische Organisationen vorhalten. Diese können für ein allgemeines Interesse, ohne Erwerbszweck, rechtlich unabhängig mit der Sammlung von Daten auf der Grundlage von Einwilligungen der die Daten hergebenden Bürgerinnen und Bürger tätig sein. Allein die EU-Kommission soll entsprechende Einwilligungsformulare/Muster in eigenem Rechtsakt vordefinieren können.

Zur Begründung wird stets auf das inzwischen im Digitale-Versorgungs-Gesetz neugeschaffene Forschungsdatenzentrum und die Verarbeitung von Daten für Forschungszwecke verwiesen. Doch der DGA-E beschränkt die Zwecke datenaltruistischer Zwecke nicht auf Forschungsinteressen, sondern hält die Definition deutlich weiter. Unklar bleiben die Abgrenzung zu den sog. Datenmittlern und die Frage, ob die Organisationen die ihnen überlassenen Daten zu eigenen Zwecken verarbeiten oder zur Weitergabe speichern. Zudem wird auch hier eine parallele Aufsichtsstruktur mit unklarem Verhältnis zu den Datenschutzaufsichtsbehörden geschaffen, obwohl in diesem Fall unzweifelhaft personenbezogene Daten betroffen sind. Kritik verdient auch die alleinige Zuständigkeit der EU-Kommission zur Erstellung von datenschutzrechtlichen Einwilligungsformularen. Hier besteht die berechtigte Sorge, dass womöglich Standards der DSGVO, etwa in Gestalt der Vorgaben zur Zweckbindung (Art. 5 Abs. 1 b. DSGVO), unterlaufen werden könnten. Das geplante sog. Europäische Einwilligungsformular sollte daher nicht als Durchführungsrechtsakt der EU-Kommission erlassen, sondern rechtsverbindlich von dem dafür kompetenten und zuständigen Europäischen Datenschutzausschuss beschlossen werden.

5. Grenzen der Einwilligung bei kollektiven Interessen

Die primär marktbezogenen Vorstellungen der Datenstrategie als auch der Entwurf des Daten-Governance-Act beim Umgang mit Big Data und den darauf laufenden Verbesserungen von Algorithmen für Entscheidungsverfahren des Alltages verstärkt den Druck auf die Ein-

willigung als die von der DSGVO nahegelegte Rechtsgrundlage. An dieser Stelle hervorgehoben, weil im Hinblick auf die zahlreichen Vorschläge der Datenethikkommission zur Algorithmenregulierung in der vorliegenden Strategie nur mit Blick auf Diskriminierung im engeren Sinne aufgegriffen, sei das Problem kollektiver Effekte von Datenanalysen. So können auf der Basis von Einwilligungen einer begrenzten Zahl von Personen Datenanalysen erstellt werden, deren Ergebnisse statistische Generalisierungen für ganze Bevölkerungsgruppen und auch die Zuordnung dieser Annahmen für diese Personengruppen erlauben, ohne dass diese entsprechend zugestimmt haben. Diese kollektive Dimension ist bereits in ähnlicher Weise aus den Verfahren von Profiling und Scoring, z.B. dem sog. Geoscoring bekannt. So kann sich etwa die Kreditwürdigkeit je nach Bewertung des Wohnortes verändern. Die erwartbare Verbreitung solcher Verfahren in den unterschiedlichsten Lebensbereichen erfordert deshalb die intensive Befassung mit den Folgen und die Weiterentwicklung der bislang allein auf individuellen Schutz ausgerichteten Schutzkonzepte des Datenschutzes. Unter dem Titel Algorithmen hat die Datenethikkommission auch hierzu zahlreiche Vorschläge vorgelegt.

6. DSGVO im Hinblick auf Algorithmen verschärfen

Moderne Datenverarbeitung ermöglicht das Anlegen, die Auswertung und Analyse ungeheurer Datenmengen aus verschiedensten Kontexten. Selbstlernende Algorithmen eröffnen immer neue Möglichkeiten, das Verhalten von Menschen vorherzusagen und sogar zu steuern. Die Verarbeitung ihrer Daten kann Betroffenen nützen, aber auch erheblich schaden. Denn beim Profiling geht es nicht nur – wie oft angenommen – um den wirtschaftlichen Nutzen im Verhältnis zu einzelnen Personen.

Die DSGVO enthält zwar eine Definition des Profilings in Art. 4 Nr. 4 und das Verbot reiner automatisierter Entscheidungsfindung in Art. 22. Sie bleibt aber letztlich vage und lückenhaft. Wir brauchen eine europäische Verschärfung des geltenden Rechtsrahmens, um die Menschen vor Manipulation und Diskriminierung wirkungsvoll zu schützen.

Die vorhandenen Regelungen der DSGVO sollten sich bereits auf die Bildung von Profilen erstrecken und nicht nur auf die automatisierte Entscheidungsfindung, die in der Praxis umgangen wird. Deshalb sollte bereits das Profiling als solches dem Verbot mit Erlaubnisvorbehalt des Art. 22 DSGVO unterstellt werden. Zudem müssen die Betroffenen generell ein Recht auf aussagekräftige Informationen haben, wenn Profilbildung stattfindet.

Nach den sachgerechten Vorschlägen der Datenethikkommission sollten verschiedene Formen der algorithmenbasierten Entscheidung - und damit unter anderem auch des Profilings - anhand ihres Risikopotentials klassifiziert und reguliert werden. Diese Klassifizierung richtet sich etwa nach dem Einsatzzweck und der Sensibilität der Daten. In jedem Fall steht der europäische Gesetzgeber vor der Aufgabe, der ungehemmten Nutzung personenbezogener Daten zur Profilbildung effektive Grenzen zu setzen und bedarf hier auch des Anschubes und der Impulse aus den Mitgliedstaaten.

7. Bezahlen mit Daten?

Mit Blick auf die laufende Umsetzung der Richtlinie Digitale Güter und Dienstleistungen verweise ich auf das Plädoyer der Datenethikkommission, die Bezeichnung von Daten als Gegenleistung weiter zu vermeiden. Im konkreten Fall der Prüfung der Rechtsgrundlagen wird sich bei entsprechenden Geschäftsmodellen weiterhin die Frage stellen, ob aus datenschutzrechtlicher Perspektive überhaupt wirksame Einwilligungen zustande gekommen sind, und ob womöglich gegen das Kopplungsverbot aus Artikel 7 Abs. 4 DSGVO verstoßen wurde. Auch bei einer vertragsbasierten Verarbeitung im Sinne von Art. 6 Abs. 1 lit. b) DSGVO sind der Vertragsfreiheit durch die zentralen Prinzipien des Datenschutzes (Art. 5 DSGVO) klare Grenzen gesetzt.

V. Medienkompetenz und Vorreiterrolle des Staates

Zu den überwiegend bereits laufenden Maßnahmen des IV. Kapitels zur Vorreiterrolle des Staates habe ich bereits in zahlreichen Fällen konkret Stellung genommen. Hervorzuheben sind an dieser Stelle erneut die grundsätzlichen verfassungsrechtlichen Bedenken gegen die Registermodernisierung in der vorliegenden Form (Stellungnahme abrufbar unter https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2020/21_Registermodernisierung.html). Dabei haben wir auch zu den guten Ansätzen für ein sog. Datencockpit Stellung bezogen.

Die geplante digitale, portalgestützte Rentenübersicht erfordert entsprechende gesetzliche Grundlagen und Vorgaben auf der Grundlage bereits eingeführter vergleichbarer Vorhaben wie den digitalen Familienleistungen.

Ulrich Kelber

Bundesbeauftragter für den Datenschutz und die Informationsfreiheit