Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Bonn, den 25.06.2024

Stellungnahme

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zur öffentlichen Anhörung des Deutschen Bundestags
- Ausschuss für Digitales -
am 26. Juni 2024
zum Thema: „Innovative Datenpolitik: Potentiale und Herausforderungen“

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

1. Kerngedanken

Die Potenziale der Nutzung von – auch personenbezogenen – Daten liegen auf der Hand. Forschungsvorhaben im Gesundheitsbereich, gemeinwohlorientierte Projekte wie Smart Cities auf kommunaler Ebene, die verbesserte Aussteuerung von Leistungen im Bereich der Daseinsvorsorge (Mobilität, Energie): diese Projekte erfordern eine Auswertung von häufig großen Datenmengen in hoher Qualität.

Damit diese Potenziale gehoben werden können, sind eine moderne Infrastruktur und moderne Technologien essentiell. Sie leisten zudem einen großen Beitrag zur datenschutzkonformen Nutzung personenbezogener Daten für die Datenökonomie.

Die DSGVO stellt klar, dass bereits beim Entwurf einer neuen Anwendung die Anforderungen des Datenschutzes mitgedacht werden müssen -- welche Daten benötige ich wirklich für mein Vorhaben? Wie kann ich mein Vorhaben so strukturieren, dass konkrete Risiken gar nicht erst entstehen, oder geeignete Schutztechnologien einsetzen, um die Risiken zu reduzieren? "Datenschutz by design" ist nicht optional, sondern zwingende Anforderung der DSGVO. Datenschutz ist konkreter Grundrechts- und Bürgerschutz. Gerade in den in der Datenökonomie häufig diskutierten Fällen der Weiterverwendung von Daten in Datenräumen müssen geeignete, risikoadäquate Technologien als technisch organisatorische Maßnahmen eingesetzt werden. Dies sind zum einem klassische Verfahren, wie etwa Anonymisierung, Pseudonymisierung und Verschlüsselung. Zum anderen sind dies auch innovative Verfahren wie Zero-Knowledge-Proofs, homomorphe Verschlüsselung, differential privacy, secure multiparty computation und ähnliches.

Wer innovative Datenverwendung fördern will, darf keine Angst vor innovativen Technologien für den Schutz der Daten haben. Eine innovative Datenpolitik muss sich aus meiner Sicht zwingend mit solcher Infrastruktur und solchen Technologien befassen, deren Entwicklung vorantreiben und deren Einsatz forcieren. Dies gilt beispielsweise für die online-Funktion des neuen Personalausweises, die noch nicht weit genug verbreitet genutzt wird.

Denn anders als es zum Teil auch manche Fragen des an uns Sachverständige gerichteten Fragenkatalogs suggerieren, steht „der Datenschutz“ einer innovativen Datenpolitik gerade nicht im Wege. Innovative Datennutzung ist auch unter dem bestehenden Rechtsrahmen möglich – wenn entsprechende technische und organisatorische Maßnahmen getroffen werden. Darüber hinaus ist Datenschutz Innovationsförderer. Datenschutz schafft Vertrauen, das Basis für eine nachhaltige Nutzung digitaler Produkte und Dienstleistungen ist.

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

Für diese Produkte ist Datenschutz ein Qualitätsmerkmal und eine starke Argumentationsgrundlage im Markt. Datenschutz schafft aber auch Vertrauen in digitale Verwaltungsstrukturen und steigert die Akzeptanz von Datennutzung bspw. zu Forschungs- oder gemeinwohlorientierten Zwecken bei jedem Einzelnen.

Dazu müssen natürlich Datenschutzprinzipien wie Datenschutz by design als Standard jedes datenbasierten Projektes mitgedacht werden. Datenschutzbehörden müssen frühzeitig beteiligt werden. Präventiver Datenschutz ist insoweit effizient und auch ökonomisch für die betroffenen Stellen die sinnvolle Lösung.

Bevor weitere Regulierung, weitere Zugangsregelungen zu Daten und weitere „Formate der Datenpolitik“ eingerichtet werden, wie das im Fragenkatalog teilweise anklingt, rege ich dringend an, die Spielräume zu nutzen, die der geltende Rechtsrahmen einräumt. Dies gilt für neue nationale Gesetze wie das Gesundheitsdatennutzungsgesetz und das Forschungsdatengesetz ebenso wie für die Umsetzung des Data Acts und des Data Governance Acts, die bereits wesentliche Ziele der Datenökonomie adressieren. Langwierige Umsetzungsverfahren auf nationaler Ebene verzögern unnötig die unter diesen Rechtsakten beabsichtigte innovative Datennutzung.

Dies gilt aber auch für die Spielräume der DSGVO im Bereich des technologischen Datenschutzes. In vielen Fällen könnten vorhandene Daten bereits heute datenschutzkonform genutzt werden, wenn entsprechende Technologien wie bspw. Anonymisierung oder PETs eingesetzt würden und eine moderne und sichere Infrastruktur zur Verfügung stünde. Ich plädiere daher noch einmal dafür, im Rahmen einer innovativen Datenpolitik einen Fokus auf Infrastruktur und Technologie zu legen, um die vorhandenen Potenziale zu heben.

2. Zu den Fragen im Einzelnen:

Hinweis: Fragen ohne datenschutzrechtliche Relevanz werden nicht berücksichtigt.

1) *Mit dem Data Act und dem Data Governance Act (und weiteren Rechtsakten) wurde ein wegweisender europäischer Datenraum geschaffen. Welche Spielräume hat der deutsche Gesetzgeber bei der Umsetzung der Vorgaben, die er für eine innovative Datenpolitik nutzen sollte und welche Maßnahmen sehen Sie bei der Umsetzung - etwa in der Bündelung der Aufsicht für die digitalpolitischen Dossiers – als besonders wichtig an?*

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

- Data Act und Data Governance Act schaffen umfangreiche Grundlagen für eine Datenbereitstellung und Datennutzung, so dass bereits deren Umsetzung und Anwendung eine spürbar innovative Datennutzung ermöglichen.
- Für die nationale Umsetzung des Data Governance Act liegt seit Anfang 2023 ein Entwurf für das Daten-Governance-Gesetz vor, der kürzlich in eine zweite Abstimmungsrunde ging – Finalisierung noch offen. Solch langwierige Verfahren stellen Hürden bei der Umsetzung dar und verzögern – unnötig – die durch den Data Governance Act ermöglichte innovative Datennutzung.
- Erste Anfragen zeigen den umfangreichen Bedarf an Abstimmung zwischen den fachspezifischen und den Datenschutz-Aufsichtsbehörden auf, soweit Datenschutzgesichtspunkte betroffen sind. Gesetzliche Vorgaben zu Beteiligungsverfahren könnten hier die Bearbeitung erleichtern, fehlen jedoch bisher – auch im Entwurf zum Daten-Governance-Gesetz.
- Die Behörden, die mit Aufgaben aus den Digitalrechtsakten betraut sind, haben daher aus eigener Initiative für eine verstärkte Zusammenarbeit das Digital Cluster Bonn gegründet. Mitglieder sind die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), das Bundesamt für Justiz (BfJ), das Bundesamt für Sicherheit in der Informationstechnik (BSI), das Bundeskartellamt (BKartA), die Bundesnetzagentur (BNetzA) und ich (BfDI) (mit eigenem Web-Auftritt: https://www.digitalcluster-bonn.de/DCB/start.html).
- Ich empfehle, in den Umsetzungsgesetzen bei der Bestimmung der zuständigen Behörden besonders die existierenden Zuständigkeiten und die tatsächlich geübte Praxis und die bei den Behörden bereits vorhandenen Kompetenzen zu berücksichtigen. Dies gilt insbesondere für die noch ausstehende Zuständigkeitszuweisung im Bereich KI, die naheliegend – entsprechend der Positionierung der DSK vom 3. Mai 2024[1] – die Datenschutzaufsichtsbehörden benennen sollte.

2) *Für eine innovative Datenpolitik bedarf es einer innovativen, modernen aber auch sicheren und vertrauenswürdigen Infrastruktur. Was sind zentrale Elemente dieser Infrastruktur, wie muss diese ausgestaltet sein, um eine innovative Datenpolitik zu ermöglichen und wie weit sind wir beim Aufbau einer solchen Infrastruktur und welche Bedeutung kommt hier einer souveränen europäischen Cloudinfrastruktur zu?*

- Der Begriff Infrastruktur ist sehr breit zu fassen. Sichere und vertrauenswürdige Infrastruktur umfasst nicht nur klassische IT-Infrastruktur im Sinne von Netzen und

[1] Positionspapier der DSK vom 3. Mai 2024 – Nationale Zuständigkeiten für die Verordnung zur Künstlichen Intelligenz (KI-VO), https://www.datenschutzkonferenz-online.de/media/dskb/20240503_DSK_Positionspapier_Zustaendigkeiten_KI_VO.pdf

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

Rechenzentren, sondern auch gemeinsamen Standards und Datenformate, wiederverwendbare Basissysteme und einheitliche Rahmenbedingungen.

- Zu den einheitlichen Rahmenbedingungen gehören etwa einheitliche Vorgaben / Anforderungen an Sicherheitsniveaus. Nur wenn alle Verwender einer Infrastruktur sich einig darüber sind, welches Sicherheitsniveau (oder welche Sicherheitsklassen) diese Infrastruktur haben soll, kann sie auch von allen sinnvoll genutzt werden. Statt einer Absenkung der Sicherheit einer Anwendung vorgeblich im Dienste der "Nutzerfreundlichkeit" sollten vielmehr gemeinsame Infrastrukturen mit einheitlichem und angemessenen Sicherheitsniveau und Nutzerfreundlichkeit geschaffen werden.
- Ein wiederwendbares Basissystem in diesem Sinne ist z.B. die elektronische Identität des Personalausweises. An diesem Beispiel ist aber auch erkennbar, dass es notwendig ist, gemeinsame Basissysteme dann auch gemeinsam zu vertreten und einzusetzen.
- Auch Datenportabilität und -wiederverwendbarkeit setzen voraus, dass die Daten in gemeinsamen und interoperablen Formaten vorliegen, die durch offene Standards definiert werden. Neben dieser technischen Interoperabilität ist aber auch wieder ein gemeinsames Verständnis von Sicherheit notwendig. Wenn ein Empfänger von Daten nicht nachvollziehen kann, auf welchem Sicherheitsniveau die Korrektheit der Daten abgesichert ist, sind die Daten wertlos. Umgekehrt muss ein Sender von Daten nachvollziehen können, dass auch beim Empfänger die Vertraulichkeit weiterhin auf dem gemeinsam vereinbarten Sicherheitsniveau gewährleistet wird. In vielen Bereichen wird dies – aufgrund der vielen Beteiligten – neben der Festlegung in offenen Standards auch regulative Vorgaben erfordern.
- Die Durchsetzbarkeit von gemeinsamen Standards wird – zumindest dort, wo ein hohes Sicherheitsniveau notwendig ist – oft auch einen gemeinsamen Rechtsrahmen voraussetzen. Insofern kommt dem Konzept einer souveränen Cloud in diesem Zusammenhang wesentliche Bedeutung zu. Die Digitalrechtsakte der EU geben uns sowohl einen Rahmen für gemeinsame Standards, als auch deren Einbettung in einen gemeinsamen Rechtsrahmen. Cloud-Infrastrukturen sind in vielen Bereichen heute nicht mehr wegzudenken. Umso wichtiger ist es, dass diese auch die (gemeinsamen) Anforderungen einhalten und dies transparent und nachweisbar ist.
- Die Datenschutzkonferenz (DSK) hat sich bereits vor einiger Zeit Gedanken dazu gemacht, welche Anforderungen eine Cloud erfüllen sollte, um als "souverän" gelten

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

zu können, aus Sicht des Datenschutzes, aber auch im Sinne der Portabilität, der Transparenz usw.[2]

- Der durch die Digitalrechtsakte eröffnete Rahmen für gemeinsame Vorgaben und Standards muss nun in gemeinsamer Arbeit unter Beteiligung aller Stakeholder gefüllt werden.

3) *Oft wird Datenschutz als Hemmnis für innovative Datenpolitik vorgeschoben oder werden Datenpolitik und Datenschutz gegeneinander in Stellung gebracht. Wie sehen Sie die Rolle des Datenschutzes für eine innovative Datenpolitik, welche Instrumente wie beispielsweise Datentreuhänder können welchen Beitrag leisten, um Datenschutz und innovative Datenpolitik zusammenzudenken und sehen Sie es auch als Wettbewerbsvorteil an, innovative Datenpolitik unter Wahrung des Datenschutzes made in EU sicherzustellen?*

- Dass Datenschutz und innovative Datennutzung sich nicht ausschließen, beweisen u.a. die Digitalrechtsakte Data Governance Act und Data Act.
- Der Data Governance Act bildet die Basis für Datenvermittlungsdienste, die je nach Ausgestaltung auch als Datentreuhandplattformen bekannt sind. Sie ermöglichen eine Datennutzung durch Dritte und zugleich die Gewährleistung des nötigen Schutzes der betroffenen Personen – oder auch von Geschäftsgeheimnissen.
- Wesentlich ist, dass der Vermittlungsdienst neutral arbeitet und kein eigenes Interesse an der Datennutzung hat und Datensicherheit gewährleistet. Zudem müssen seine Aufgaben klar umrissen sein.
- Zum Service kann – als Instrument zum Schutz der betroffenen Personen – die Pseudonymisierung, die Anonymisierung oder die sonstige datenschutzfreundliche Aufbereitung der personenbezogenen Daten gehören.
- Der Data Governance Act bildet darüber hinaus die Basis, um Daten, die wegen gesetzlicher Regelungen besonders geschützt sind (z.B. Datenschutzrecht), und daher grundsätzlich von der Weiterverwendung ausgeschlossen sind, nutzen zu können. Dazu werden zusätzliche Anforderungen genannt, wie eine sichere Verarbeitungsumgebung, Anonymisierung, Aggregierung oder vertragliche Geheimhaltungsverpflichtungen.
- Datenschutz by design ist zwingende Anforderung der DSGVO. Innovative Datenpolitik muss sich daher auch mit risikoadäquaten technisch-organisatorischen Maßnahmen gem. Art. 25, 32 DSGVO befassen, wie etwa PETs – innovative Datenverwendung bedarf innovativer Lösungen zum Schutz der betroffenen Personen.

[2] Positionspapier der DSK vom 11. Mai 2023 – Kriterien für Souveräne Clouds, https://datenschutzkonferenz-online.de/media/weitere_dokumente/2023-05-11_DSK-Positionspapier_Kritierien-Souv-Clouds.pdf

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

- Auch im nationalen Recht gibt es bereits Regelungen, die eine Nutzung von Daten im Einklang mit den datenschutzrechtlichen Anforderungen ermöglichen, wie z.B. § 16 BStatG für Daten beim Statistischen Bundesamt für wissenschaftliche Forschung, oder die Datentransparenzregelungen in §§ 303a ff SGB V (Forschungsdatenzentrum beim BfArM) für weitere Zwecke.
- Im Übrigen wird die elementare Bedeutung der datenschutzrechtlichen Regelungen, also des wirksamen Schutzes des Persönlichkeitsrechts, auch in anderen Regionen der Welt gesehen und es werden an der DSGVO orientierte Gesetze erlassen. Datenschutz stellt unzweifelhaft ein Qualitätsmerkmal in der modernen Welt dar, so dass Datenschutzkonformität durchaus einen Wettbewerbsvorteil bietet.
- Immer dann, wenn frühzeitig die Anforderungen des Datenschutzes bei der Konzipierung eines Produkts oder auch eines Gesetzes mitgedacht werden, oder wenn ich frühzeitig beratend eingebunden werde, sind die Datenschutzvorgaben meist leicht zu implementieren. Als Hemmnis erweisen sich datenschutzrechtliche Anforderungen allerdings oft dann, wenn sie zu spät gesehen oder wegen einer späten Einbindung erst im fortgeschrittenen Entwicklungsstadium von mir eingebracht werden können und umfangreiche Nachbesserungen bedingen – ein vermeidbares Problem also.

5) *Haben Forschung, Zivilgesellschaft und öffentliche Stellen ausreichend Datenzugang zu den Daten sehr großer Online-Plattformen (VLOPs) und anderen datenhaltenden Unternehmen, um gemeinwohlorientierte Fragestellungen zu Themen wie beispielsweise Klimaschutz, sozialer Gerechtigkeit oder effizienter Verwaltung zu bearbeiten bzw. gibt es weitere Ansatzpunkte im nationalen und EU-Recht, um einen solchen Datenzugang zu gewährleisten und welchen Regelungsbedarf sehen Sie insoweit für die Zukunft?*

- Entsprechend meiner Aufgabe beschränke ich mich hier auf den Zugang zu personenbezogenen Daten.
- Es gibt inzwischen eine Vielzahl von Datenzugangsansprüchen, insbesondere für die wissenschaftliche Forschung:
    - Die Datentransparenzregelungen in §§ 303a ff SGB V für die Abrechnungsdaten der Krankenkassen beim Forschungsdatenzentrum (FDZ) Gesundheit beim Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM): Durch die Abkehr vom abschließenden Katalog von benannten Berechtigten hin zu einem zulässigen Zweck als Antragsvoraussetzung wird der Zugang prinzipiell für jeden eröffnet. Die betroffenen Personen werden über verschiedene Nutzungsbedingungen geschützt (Antragsprüfung, Datenauswahl, Pseudo-

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

nymisierung). Das Gesundheitsdatennutzungsgesetz unterstützt die gemeinwohlorientierte Forschung und fördert Innovationen durch Einrichtung einer zentralen Datenzugangs- und Koordinierungsstelle für Gesundheitsdaten beim BfArM mit einem Metadatenkatalog und einem Antragsregister. Außerdem ermöglicht es – unter bestimmten Bedingungen - die Verknüpfung der Daten des Forschungsdatenzentrums (§§ 303a ff SGB V) mit denen der Krebsregister der Länder.
    - § 16 Abs. 6 BStatG: Zugang für unabhängige wissenschaftliche Forschung zu faktisch anonymisierten Einzeldatensätzen oder in sicherer Verarbeitungsumgebung („innerhalb speziell abgesicherter Bereiche“)
    - Art. 40 Abs. 4 Digital Services Act sieht einen Datenzugang zu Daten von Very Large Online Platforms / Search Engines (VLOP, VLOSE) für Forscher vor – auf Verlangen des Koordinators für Digitale Dienste / Digital Services Coordinator (DSC: BNetzA) / auf Antrag der Forscher unter den Voraussetzungen des Art. 40 Abs. 8 DSA (u.a. bestimmte Thematik)
    - Das BMBF plant ein Forschungsdatengesetz, das u.a. mittels Anpassungen im Bundesstatistikgesetz Zugang zu amtlichen Daten gibt. Ein Micro Data Center soll als One-Stop-Shop Daten aus verschiedenen Quellen zusammenführen.
- Beispielhaft weitere Zugangsansprüche – unabhängig von Forschung:
    - Art. 6 Data Governance Act für die Weiterverwendung von geschützten behördlichen Daten, also die, die vom Zugangsanspruch nach IFG gerade ausgeschlossen sind – unter bestimmten Maßgaben zum Schutz der betroffenen Personen
    - Art. 4 Data Act: für die Nutzer von vernetzten Produkten und verbundenen Diensten: Zugang zu den von ihnen / bei der Nutzung generierten Daten; und Art. 5 Data Act: auf Verlangen der Nutzer Zugang für Dritte unter bestimmten Bedingungen, insbesondere Wahrung des Datenschutzes und von Geschäftsgeheimnissen. Dabei verlangt Art. 11 Data Act besondere technische Schutzmaßnahmen.
    - Art. 14 Data Act gibt öffentlichen Stellen einen Anspruch gegenüber Dateninhabern auf Datennutzung bei einer außergewöhnlichen Notwendigkeit im öffentlichen Interesse.
- Diese zum Teil recht neuen Normen geben teilweise umfassende Zugangsmöglichkeiten. Erst nach der Umsetzung und Ausschöpfung dieser Regelungen wird sich zeigen, ob und was darüber hinaus als erforderlich angesehen wird.

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

- Zum Schutz der betroffenen Personen bedarf es dabei des Bewusstseins, dass das Grundrecht auf Datenschutz sowohl auf nationaler Ebene – als Grundrecht auf informationelle Selbstbestimmung – als auch auf europäischer Ebene in Art. 8 der Grundrechtecharta verankert ist. Einschränken dürfen nach Art. 52 der Grundrechtecharta nur unter Wahrung des Grundsatzes der Verhältnismäßigkeit nur vorgenommen werden, wenn sie den anerkannten dem Gemeinwohl dienenden Zielsetzungen oder dem Schutz anderer entsprechen.
- Dieser Gemeinwohlbezug ist – neben dem Vertrauen in eine sichere Verarbeitung – wesentlich für eine Akzeptanz der Betroffenen bei der Nutzung ihrer personenbezogenen Daten.

6) *Welchen Effekt haben neue Formate der Datenpolitik wie das von BMWK und BMI vorangetriebene Dateninstitut für eine innovative Datenpolitik und braucht es weitere Maßnahmen, um eine breite Nutzung von Daten für das Wohl der Gesellschaft zu ermöglichen?*

- Ein Dateninstitut, das Datenverfügbarkeit und –standardisierung sektorübergreifend vorantreibt, Datentreuhändermodelle und Lizenzen etablieren soll, kann wertvolle Impulse zur datenschutzkonformen Datennutzung geben.
    - Datentreuhändermodelle können das Teilen von Daten erleichtern, Aktivitäten der Treuhänder müssen aber klar umrissen und Interessenkonflikte ausgeschlossen werden. Die Anforderungen des Data Governance Acts an Datenvermittlungsdienste müssen dabei berücksichtigt werden. Technologien zur Aufbereitung der personenbezogenen Daten, wie etwa Anonymisierungstechniken oder aber PETs, müssen geprüft und stetig weiterentwickelt werden.
    - Bei Standardisierung und Labelling ließen sich auch datenschutzfreundliche Automatismen entwickeln (bspw. Labels mit passenden Löschfristen, Verarbeitungsbedingungen oder ähnliches).
- Das Dateninstitut sollte – auch im Falle etwaiger allgemeiner Beratungstätigkeit – nicht als Antipode zu den Datenschutzbehörden agieren. Die abschließende datenschutzrechtliche Beurteilung von Use Cases muss durch die Datenschutzbehörden erfolgen.
- Konkrete Effekte des Dateninstituts lassen sich noch nicht bewerten. So soll im laufenden Gründungsprozess etwa noch das konkrete Aufgabenspektrum des Instituts skizziert werden. Unabhängig von weiteren neuen Formaten der Datenpolitik sollte

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

aus Datenschutzsicht ein Schwerpunkt auf privacy by design, Anonymisierung/Pseudonymisierung und PETs gelegt werden, um eine datenschutzkonforme „breite Nutzung von Daten für das Wohl der Gesellschaft“ zu ermöglichen.

7) *Welche Form der Zusammenarbeit ist auf internationaler Ebene notwendig, um eine innovative Datenpolitik proaktiv und menschenzentriert voranzutreiben und Bedeutung kommt dabei dem sogenannten „globalen Süden“ zu?*

- Besonders wichtig für die Zusammenarbeit auf internationaler Ebene ist die aktive Teilnahme und Präsenz in relevanten internationalen Foren und Gruppen, um Einfluss auf Diskussionen zu Themen von globaler Bedeutung nehmen zu können. Hierzu gehören etwa der freie und sichere grenzüberschreitende Datenverkehr (DFFT), Künstliche Intelligenz oder Government Access.
- Ich bin daher in allen wichtigen internationalen Foren der Datenschutzbehörden (DPAs) aktiv und nehme dort eine führende Rolle ein. Herauszustellen sind der G7 DPA Roundtable, die Global Privacy Assembly, die OECD (Working Party on Data Governance and Privacy, DGP), der Europarat (Beratender Ausschuss zu Konvention 108, T-PD), das Global CBPR Forum (hier bin ich bisher als einzige EU-DPA beratend aktiv) oder die Berlin Group.
- Der offene Dialog mit Partnern aus unterschiedlichen Jurisdiktionen ist entscheidend, um global hohe Datenschutzstandards zu fördern und sichere Drittstaatentransfers zu ermöglichen. In Ländern des „globalen Südens“ bestehen oftmals keine oder nur geringschwellige Datenschutzregime. In der Zusammenarbeit mit dortigen Behörden sollte daher die (auch wirtschaftliche) Bedeutung robuster Datenschutzregelungen betont werden.
- Ich kooperiere im Rahmen internationaler Foren wie etwa der Global Privacy Assembly oder dem Europarat mit diversen DPAs des „globalen Südens“ und suche besonders engen Kontakt zu DPAs mit einer Schlüsselrolle in ihrer jeweiligen Region (etwa CNDP Marokko als permanentes Sekretariat des Network of African Data Protection Authorities, NADPA).

10) *Die Bundesregierung hat im Jahr 2023 eine überarbeitete Datenstrategie veröffentlicht (https://www.bundesregierung.de/breg-de/themen/digitalisierung/datenstrategie-2023-2216620). Wie beurteilen Sie diese in ihrer Machart und Zielsetzung und in ihrer bisherigen Umsetzung?*

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

- Ich habe im Rahmen der Ressortbeteiligung mehrfach Stellung zur Datenstrategie genommen. Einige meiner Anregungen haben in die Datenstrategie Eingang gefunden.
- Zu begrüßen ist, dass die Datenstrategie Bekenntnisse zum bestehenden, auch europäischen Datenschutzstandard enthält. Dennoch wird der Bedeutung des Datenschutzes in der Datenstrategie nicht ausreichend Rechnung getragen. Es verbleibt der Eindruck, Datenschutz(recht) sei primär ein Hindernis für angestrebte Datennutzungen und könnte durch kluge Strategien überwunden, umgangen oder relativiert werden. Das in der Strategie genutzte Vokabular trägt bei zu dem Eindruck einer beliebigen Handelbarkeit von personenbezogenen Daten, die abzulehnen ist.
- Datenschutz ist nicht innovationshemmend, sondern im Gegenteil ein neuralgischer Punkt der Digitalisierung und ein vertrauensbildendes Qualitätsmerkmal für Produkte, Dienstleistungen und Verwaltungsleistungen.
- Die DSGVO ermöglicht bereits die Umsetzung innovativer datengetriebener Verwaltungsaktivitäten bzw. Geschäftsmodelle – unter Einsatz entsprechender technischer und organisatorischer Maßnahmen. Der Gesetzgeber kann entsprechende Öffnungsklauseln nutzen, wie dies in der Datenstrategie auch vorgesehen ist.
- Technische und organisatorische Maßnahmen, die in der Datenstrategie benannt sind, können einen großen Beitrag zur datenschutzkonformen Datennutzung leisten (bspw. Datenschutzcockpits, Datentreuhänder, PIMS, PETs, Anonymisierung).
- Bei Standardisierung und Labelling, wie in der Datenstrategie vorgesehen, ließen sich auch datenschutzfreundliche Automatismen entwickeln (bspw. Labels mit passenden Löschfristen, Verarbeitungsbedingungen o.ä.).
- Die Datenstrategie gibt keine Antwort auf die grundlegende Frage, 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 eher die Erstreckung weiterer gesetzlicher Datenschutzvorkehrungen zum Schutz der Bürgerinnen und Bürger auch auf den Umgang mit nicht-personenbezogenen Daten nahe.
- Die Umsetzung vieler in der Roadmap der Datenstrategie genannten Vorhaben hat bereits begonnen bzw. ist (weit) fortgeschritten (bspw. GDNG, BDSG-ÄndG).
- Darüber hinaus müssen einzelne Vorhaben, die auf die übergeordneten Ziele der Datenstrategie einzahlen (bspw. verbesserte Auffindbarkeit, Datenpools, Labelling), konkret datenschutzrechtlich begleitet werden, sofern personenbezogene Daten betroffen sind. Ich werbe dafür, Datenschutzthemen (wie bspw. privacy by design) von Beginn an mitzudenken und die Datenschutzaufsichtsbehörden möglichst frühzeitig einzubeziehen.

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

- Auf Durchsetzungsebene – wie etwa bei der Umsetzung des Data Act bzw. des Data Governance Acts, der KI-Verordnung oder anderer Digital- bzw. Datenrechtsakte, die in weiten Teilen noch aussteht – müssen Kooperationsregelungen zwischen Daten-schutz- und sonstigen beteiligten Behörden getroffen und Rechtsgrundlagen für den Datenaustausch zwischen diesen Behörden geschaffen werden, um eine effektive Rechtsdurchsetzung sicherzustellen.

11) *Wie sollte, vorangestellt die Zielparameter einer verbesserten Datenverfügbarkeit- und Nutzbarkeit, eine grundlegende Neuordnung der Datenschutzaufsicht in Deutschland aussehen, wo genau sollte eine Reform der DSGVO ansetzen und welche möglichen Restriktionen sehen Sie hierbei?*

- Die DSGVO ermöglicht bereits die Umsetzung innovativer datengetriebener Aktivitäten – unter Einsatz entsprechender technischer und organisatorischer Maßnahmen; der Gesetzgeber kann entsprechende Öffnungsklauseln nutzen.
- Der Schutz der informationellen Selbstbestimmung betroffener Personen ist Zielparameter der DSGVO und Aufgabe der Datenschutzaufsicht. Auch gehört der freie Datenverkehr innerhalb der EU zwar zum Schutzzweck der DSGVO, dient hier aber dem binnenmarktorientierten Anspruch, dass in allen EU-Mitgliedstaaten dieselben Bedingungen gelten müssen und Datenaustausch innerhalb der Union von den Mitgliedstaaten keiner gesonderten datenschutzrechtlichen Beschränkung unterworfen wird. Die Sicherstellung von Datenverfügbarkeit und -nutzbarkeit als allgemeines Prinzip der Datenökonomie ist hingegen nicht unmittelbarer Zielparameter der DSGVO. Diese Schutzstandards der DSGVO dürfen nicht abgesenkt, diese Aufgabe der Datenschutzaufsicht darf nicht verwässert werden
- Aus meiner Sicht besteht durchaus Reformbedarf der DSGVO, allerdings in anderen Punkten: zum Beispiel beim langsamen prozessualen Kohärenzmechanismus, bei unzureichenden Regelungen zu Profilbildung und automatisierten Entscheidungen, es fehlt eine Herstellerhaftung, und es besteht eine impraktikable Bürokratisierung bei Informationspflichten im Rahmen der Datenerhebung.
- Die Struktur der Datenschutzaufsicht in Deutschland folgt der vom Grundgesetz vorgegebenen föderalen Struktur. Die Rechtsordnung selbst setzt hier einer grundlegenden Veränderung der Aufsichtsstruktur – etwa durch stärkere Zentralisierung beim BfDI – Grenzen. Die Zusammenarbeit zwischen mir und den Landesdatenschutzbehörden erfolgt seit vielen Jahren vertrauensvoll und mit steigender Intensität und Effektivität. Die DSK hat sich als Koordinierungsgremium bewährt, gleichwohl jedoch in ihren Planungen einer DSK 2.0 u.a. Verbesserungsmöglichkeiten der

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

Zusammenarbeit geprüft. Damit zeigt sie das verstärkte Bestreben, einheitliche Auffassungen zu erreichen

- Der Gesetzentwurf der Bundesregierung „zur Änderung des Bundesdatenschutzgesetzes“ enthält mit § 16a eine Regelung zur Institutionalisierung der DSK im BDSG. Eine Regelung zur rechtlichen Verbindlichkeit von Beschlüssen der DSK wird darin nicht getroffen.

12) *Wie kann die Umsetzung von Data Act und AI Act, gerade was die Ermöglichung von KI angeht, durch Standardisierungsarbeiten, Codes of Conducts und Codes of Practices erleichtert werden, insbesondere mit Bedeutung von Transparenz und Kontrolle über Daten?*

- Der Standardisierung kommt im AI Act eine wichtige Rolle zu (Art. 40, 41 AI Act), um konkrete Vorgaben flexibler an die schnellen technischen Entwicklungen anpassen zu können.
- Für Entwickler und Anbieter von KI bieten Standards dieser Art eine erhöhte Rechtssicherheit, wodurch Innovation gefördert werden kann. Denn bei KI-Systemen, die mit harmonisierten Normen übereinstimmen, wird eine Konformität mit diversen Anforderungen des AI Acts vermutet. Dies umfasst Transparenz und Kontrolle über Daten, aber auch beispielsweise Risikomanagement und Cybersicherheit.
- Wegen der großen Bedeutung der Standardisierung bei der Umsetzung des AI Act ist es wichtig, dass alle Interessenträger an den Standardisierungsarbeiten beteiligt sind.
- Der Data Act sieht in Art. 33 ff für Teilnehmer an den Datenräumen umfangreiche Anforderungen an die Interoperabilität vor, für die die Kommission delegierte Rechtsakte erlassen kann. Dabei berücksichtigt sie die den Rat des Europäischen Innovationsrates (EDIB, European Data Innovation Board), der gem. Art. 29, 30 Data Governance Act eingesetzt wurde. Im EDIB wirke auch ich als Vertreter des EDSA mit. Erste Beratungen zur Standardisierung haben dort bereits stattgefunden. Daher ist wichtig, dass die dort beteiligten zuständigen Behörden ihre Belange ebenso einbringen wie die Datenschutzbehörden über den EDSA die datenschutzrechtlichen Belange.

14) *Wie müssten ideale Leitlinien für die rechtssichere Anonymisierung von Daten im Rahmen der DSGVO und des Data Acts aus Ihrer Sicht ausgestaltet sein? Wie wird die Anonymisierung in anderen EU-Mitgliedsstaaten gehandhabt, und welche Maßnahmen sind erforderlich, damit Deutschland in diesem Bereich endlich Fortschritte erzielt?*

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

- Trotz ihrer hohen praktischen Bedeutung ist die Anonymisierung gesetzlich nicht klar geregelt. In der DSGVO finden wir die Definition von anonymen Informationen lediglich im Erwägungsgrund 26. Demnach sind Informationen anonym, wenn sie sich „nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen".
- Für anonyme Daten ist die DSGVO nicht anwendbar – dies ist auch die Motivation hinter den meisten Fragen zum Thema Anonymisierung: eine Verarbeitung von Daten soll nicht mehr der DSGVO unterfallen, weil die verarbeitenden Stellen die Anforderungen der DSGVO als zu einschränkend empfinden. Diese Motivation ist zwar einerseits bis zu einem gewissen Grad verständlich, aber andererseits auch sehr bedauerlich, denn die Anforderungen des Datenschutzes bestehen aus gutem Grund.
- Anonymisierung schafft Freiräume für Forschung, Wertschöpfung und Innovation. Damit ist sie ein mächtiges Instrument. Doch Anonymisierung ist oft nicht einfach. Denn es wird gleichzeitig auch versucht, den größtmöglichen Erklärungsgehalt der Daten zu bewahren: Nutzen und Werthaltigkeit von Daten auf der einen, Schutz der Menschen auf der anderen Seite. Die Komplexität einer solchen Aufgabe wird oft unterschätzt. Und auch in grundlegenden Fragen zu Anonymisierung besteht häufig noch Unsicherheit.
- Für die Anonymisierung personenbezogener Daten gibt es eine Reihe unterschiedlicher Verfahren. Die technischen Details eines effektiven Anonymisierungsverfahrens unterscheiden sich abhängig vom Einzelfall. Je nach Inhalt und Format der Daten kann ein Verfahren oder ein Parameter für einen Anwendungsfall geeignet sein, für einen anderen jedoch völlig ungeeignet. Daher ist bereits die Auswahl des richtigen Verfahrens ist eine anspruchsvolle Aufgabe, für deren korrekte Lösung viele Parameter berücksichtigt werden müssen, die stark vom jeweiligen Anwendungsfall abhängen. Dies ist ein wichtiger Unterschied zu anderen Technologien, wie etwa sicheren Verschlüsselungsverfahren, die unabhängig von der Art und Beschaffenheit der Daten funktionieren.
- Allgemeingültige Leitlinien für „rechtssichere Anonymisierung" sind aus diesem Grund zum aktuellen Zeitpunkt vor allem mit Blick auf das Adjektiv „rechtssicher" schwer denkbar. Es gibt allerdings bereits seit 2014 ein Leitliniendokument[3] der Artikel-29-Arbeitsgruppe (des Vorläufergremiums des Europäischen Datenschutzausschusses (EDSA)), das eine Reihe von Anonymisierungstechniken anhand verschiedener Kriterien vergleicht und Hinweise zu deren Vor- und Nachteilen sowie typischen Fehlerquellen gibt. Dieses Dokument wird aktuell vom EDSA grundlegend ak-

[3] Stellungnahme 5/2014 zu Anonymisierungstechniken der Artikel-29-Datenschutzgruppe; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf

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

tualisiert und erweitert und durch einen zusätzlichen Teil zu Pseudonymisierungstechniken ergänzt. Sowohl das vorhandene Dokument der Artikel-29-Gruppe als auch die kommende Aktualisierung/Erweiterung durch den EDSA bilden die gemeinsame Arbeitsgrundlage aller europäischer Datenschutzaufsichtsbehörden, und sorgen zu für eine harmonisierte Auslegung der DSGVO im europäischen Wirtschaftsraum.

- Für den Zuständigkeitsbereich des BfDI gibt es darüber hinaus seit 2020 ein Positionspapier[4], das sich spezifisch mit Fragen zur Anonymisierung im Bereich der Telekommunikationsbranche befasst.

- An dieser Stelle sei darauf hingewiesen, dass es dann, wenn es um Freiräume für Forschung, Wertschöpfung und Innovation geht, nicht immer notwendig sein muss, personenbezogene Daten komplett zu anonymisieren. Auch für den Umgang mit personenbezogenen Daten gibt es Techniken, die es ermöglichen, Daten auf sichere Art und Weise so zu nutzen, dass sowohl der Nutzen für die verarbeitenden Organisationen und der Schutz der Rechte und Freiheiten der Personen, um deren Daten es geht, gewahrt bleiben. Zu diesen sogenannten Privacy Enhancing Technologies (PETs) zählen beispielsweise Techniken wie Zero-Knowledge-Proofs, homomorphe Verschlüsselung, Differential Privacy und Secure Multiparty Computation. Wer innovative Datenverwendung fördern will, darf keine Angst vor innovativen Technologien für den Schutz der Daten haben.
- Spezifisch für Deutschland gibt es aus meiner Sicht keine besonderen Maßnahmen, die gegenüber den europäischen Leitlinien einen entscheidenden Vorteil versprechen würden. Es wäre allerdings denkbar, dass durch eine verstärkte Förderung sowohl grundlagen- als auch anwendungsorientierter Forschung zu Anonymisierungstechniken Fortschritte erzielt werden könnten, da auf diesem Weg für Verantwortliche mehr Klarheit geschaffen werden könnte, welche Verfahren mit welchen Parametern für bestimmte Einsatzszenarien gut einsetzbar sind. Dies gilt auch für Forschung und Entwicklung im Bereich der Privacy Enhancing Technologies.
- Entsprechende Projekte würden sicherlich auch die zuständigen Aufsichtsbehörden gerne im Rahmen ihrer Möglichkeiten beratend begleiten. Auch hier gilt der Hinweis, dass innovative Datenverwendung nicht unbedingt Anonymisierung benötigt, sondern durchaus auch mit Hilfe innovativer Technologien aus dem Bereich PETs möglich gemacht werden kann.

[4] Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche; https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Konsultationsverfahren/1_Anonymisierung/Positionspapier-Anonymisierung.pdf?__blob=publicationFile&v=4

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

15) *Inwiefern sind die Zweifel an der Rechtssicherheit des Data Protection Agreements zwischen den USA und der EU, das auf zwei vorhergehend aufgehobene Agreements nach dem Schrems I- und Schrems II-Urteil des EuGH folgte, berechtigt und außerdem eine Bremse für Innovationen in Europa und welche Regulierung bräuchte es, um nachhaltig für Rechtssicherheit zu sorgen?*

- Der Angemessenheitsbeschluss zum EU-US Data Privacy Framework (im Folgenden: DPF) führt für Betroffene und Datenexporteure jetzt erst einmal zu Rechtssicherheit, denn Datenübermittlungen aus der EU an nach dem DPF zertifizierte Unternehmen in die USA sind hiernach seit dem 10. Juli 2023 nunmehr wieder verlässlich möglich. Und zwar, ohne dass zusätzlichen Übermittlungsinstrumente nach Art. 46 DSGVO oder zusätzliche Maßnahmen („Supplementary measures“) im Sinne des Schrems II Urteils erforderlich wären.
- Nach meinen Erfahrungen aus der Datenschutzpraxis kann ich sagen, dass sich mit dem DPF die Lage entspannt hat und ich eine „Bremse für Innovationen“ durch das DPF nicht sehe. Vielmehr leistet das DPF einen wesentlichen Beitrag dazu, dass Daten rechtssicherer aus der EU in die USA fließen und Innovationen vorangetrieben werden können.
- Im Hinblick auf die angesprochenen Zweifel an der Rechtssicherheit, lassen Sie mich Folgendes sagen: Die Beantwortung der Frage, ob der Angemessenheitsbeschluss dauerhaft Rechtssicherheit schaffen wird, wird aller Voraussicht nach der EuGH entscheiden müssen. Dabei möchte ich darauf hinweisen, dass ein „angemessenes Schutzniveau“ nicht bedeutet, dass das europäische Datenschutzrecht 1:1 vom Drittland übernommen werden muss. Erforderlich ist ein Schutzniveau, welches dem der EU im Wesentlichen entspricht. Dies wurde mit dem DPF aus Sicht der Europäischen Kommission erreicht.
- Trotz der grundsätzlich positiven Bewertung des Angemessenheitsbeschlusses der Europäischen Kommission zum DPF durch den Europäischen Datenschutzausschuss (EDSA) sieht dieser in seiner Stellungnahme vom 28.02.2023 noch Verbesserungspotential für den kommerziellen Teil des DPF z. B. im Bereich der Weiterübermittlung (denn auch bei Weiterübermittlungen darf das Schutzniveau nicht untergraben werden) oder bei automatisierten Entscheidungsfindungen oder der Erstellung von Profilen.
- Im Bereich des Government Access, also der Frage des Zugriffs von Behörden des Drittstaates auf übermittelte Daten aus der EU zu Zwecken der nationalen Sicherheit oder der Strafverfolgung, hat der EDSA insbesondere Bedenken bzw. Klarstellungsbedarf

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

- zu den Regeln für die Datenspeicherung und -löschung sowie zur Weiterübermittlung an andere Behörden
- im Hinblick auf das Fehlen einer unabhängigen Vorab-Kontrolle sowie einer systematischen ex post Überprüfung durch ein Gericht oder eine andere unabhängige Stelle bei sog. „Bulk Collections“. Gerade die unabhängige Vorab-Kontrolle ist nach der jüngeren Rechtsprechung des EGMR eine notwendige Voraussetzung für „Bulk Collection“.
- sowie zu den standardisierten Antworten an die Beschwerdeführer.

- Ein Schutzmechanismus zur Überprüfung der Funktionsweise eines jeden Angemessenheitsbeschlusses ist gem. Art. 45 Abs. 3 DSGVO vorgesehen, wonach der Beschluss mindestens alle vier Jahre zu überprüfen ist. Die Europäische Kommission hat eine erste Überprüfung des Angemessenheitsbeschlusses zum DPF bereits nach einem Jahr vorgesehen. Dieser erste sogenannte Review zum DPF findet nun im Juli 2024 statt. Hieran werden der EDSA und auch der BfDI beteiligt sein. Wir werden die Funktionsweise des DPF auf den Prüfstand stellen und mit der US Seite in Austausch treten.
- Was die Frage nach einer neuen oder zusätzlichen Regulierung betrifft, sehe ich keine Notwendigkeit, da die DSGVO bereits das „Handwerkszeug“ bereithält, um freie Datenflüsse zu ermöglichen. Ob die faktischen Bedingungen im Drittland dann einem angemessenen Datenschutzniveau i. S. d. DSGVO entsprechen, muss sich an den rechtlichen Gegebenheiten messen lassen.

16) *Wie können Innovationen sowohl im Bereich digitaler Dienste als auch im Bereich Regulierung für mehr Datenschutz und Einhaltung der Grundrechte sorgen und welche guten Beispiele kennen Sie dafür?*

- Fortschritte und Weiterentwicklungen bei Anonymisierungs- und Pseudonymisierungskonzepten, bei Privacy Enhancing Technologies (PETs), bei datenschutzbezogenen Datentreuhandmodellen, beim Einwilligungsmangement sowie bei dezentraler Datenhaltung und Datenportabilität können neu entstehende Gefährdungen der Persönlichkeitsrechte zum Teil einhegen oder kompensieren helfen.

17) *Was kann und sollte Ihrer Auffassung nach der Staat tun, damit die Datenbestände, über die er selbst auf Bundes-, Landes- und kommunaler Ebene verfügt, nicht weiterhin unberührt in Silos schlummern, sondern von der Gesellschaft insgesamt besser genutzt werden können, etwa zum Bürokratieabbau, zu mehr Sicherheit und Komfort beim Nutzen*

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

staatlicher Leistungen? Wäre vor diesem Hintergrund das Zusammenlegen einzelner Datenbanken zu einem großen Register ein vernünftiger Weg, und falls ja, wie ließe sich dieser verfassungsfest im Sinne des Föderalismus beschreiten?

- Die Nutzung (Weiterverwendung) von Daten bei öffentlichen Stellen wird bereits im Data Governance Act adressiert und umfangreich ermöglicht. Es hängt also von der Ausschöpfung dieser Möglichkeiten ab, wie die Daten genutzt werden können.
- Wesentlich im Hinblick auf personenbezogene Daten ist das Implementieren der vorgesehenen Schutzmechanismen wie Anonymisierung, Anwenden von PETs oder das Einrichten sicherer Verarbeitungsumgebungen.
- Im Entwurf des Daten-Governance-Gesetzes ist das Statistische Bundesamt als zuständige Behörde (im Sinne des Art. 7 DGA) für die Beratung der öffentlichen Stellen hinsichtlich der Weiterverwendung ihrer Daten vorgesehen. Zu den Aufgaben gehört ggf. auch die Entscheidung über die Weiterverwendung und die Leistung technischer Unterstützung durch die Bereitstellung einer sicheren Verarbeitungsumgebung.
- Hier kommt es also auf eine zügige nationale Umsetzung und praktische Anwendung der bereits existierenden europäischen Normen an.

- Eine Zentralisierung bietet nach heutigem Stand der Technik keinen Vorteil, wenn die Standards interoperabel sind. Eine Zentralisierung schafft regelmäßig zusätzliche Risiken und erhöht den Aufwand für die Datensicherheit. Zudem wird das Zweckbindungs- und Erforderlichkeitsprinzip häufig der zentralen Zusammenführung entgegenstehen, jedenfalls soweit damit eine Verdoppelung verbunden ist.
- Wesentlich ist Transparenz z.B. über ein Registerverzeichnis mit Metadaten, um Datennutzenden einen guten Überblick zu geben, wo die für sie sinnvollen Daten vorgehalten werden und unter welchen Bedingungen Zugang besteht.
- Die Nutzung der von öffentlichen Stellen gehaltenen personenbezogenen Daten bedarf dann – unabhängig davon, ob sie verteilt gespeichert, temporär oder dauerhaft zentral zusammengeführt sind – einer Rechtsgrundlage sowie weiterer Voraussetzungen wie etwa der Transparenz für die davon Betroffenen.

18) *Die großen Digitalkonzerne zeigen es: Maschinenlesbare Daten haben einen Wert, mit ihrer Monetarisierung werden die zahlreichen Dienste, die unseren Alltag prägen, finanziert. Sollten Ihrer Auffassung nach digitale Daten, die die Menschen alltäglich erzeugen und die gleichsam als Blut der Gesellschaft zirkulieren, auch offiziell einen Wert und damit einen Preis bekommen, und wenn ja, wie ließe sich eine solche Datenökonomie im*

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

Wortsinn aufbauen und regulieren? Wie ließe sich die griffige Formel vom „Eigentum an den eigenen Daten“ real umsetzen?

- Aus datenschutzrechtlicher Sicht ist das Konzept des „Dateneigentums“ im Hinblick auf personenbezogene Daten abzulehnen. Dateneigentum würde bedeuten, personenbezogene Daten als privatwirtschaftliches Handelsgut zu betrachten. Die Achtung des Privatlebens, der Schutzes personenbezogener Daten und das Recht auf informationelle Selbstbestimmung sind Grundrechte, die letztlich einen immateriellen Kern haben und deren Berücksichtigung und Ausübung deshalb keinen Preis haben dürfen. Eine betroffene Person kann zwar der Verarbeitung ihrer personenbezogenen Daten zustimmen, sie kann jedoch nicht auf ihre entsprechenden Grundrechte verzichten. Vor diesem Hintergrund stellt auch der EDSA regelmäßig etwa in Stellungnahmen zu Europäischen Digitalrechtsakten klar, dass personenbezogene Daten kein Handelsgut sind. Auch die Datenethikkommission lehnt das Konzept des Dateneigentums ab.
- Die Hoheit betroffener Personen über die eigenen personenbezogenen Daten muss auch in der Datenökonomie berücksichtigt werden. Dazu gehören neben den Transparenzanforderungen insbesondere die Ausübung der datenschutzrechtlichen Betroffenenrechte (bspw. Erteilung bzw. Widerruf von Einwilligungen/Widerspruch/Löschung). Hierzu können Instrumente wie Datenschutzcockpits oder Datentreuhänder (bspw. PIMS) beitragen, die das Potential haben, den Einzelnen zur besseren Ausübung der Datenschutzrechte zu befähigen. Besonders wichtig sind in diesem Zusammenhang allerdings die rechtlich klar umrissene Aufgabe eines Datentreuhänders ebenso wie der Ausschluss von Interessenkonflikten.
- Natürlich hat die Nutzung von personenbezogene Daten faktisch einen wirtschaftlichen Wert und wird bspw. zur Finanzierung von digitalen Diensten genutzt, wie etwa zum Ausspielen verhaltensbezogener Werbung. Auch hierbei muss jedoch dem Recht auf Schutz der personenbezogenen Daten Rechnung getragen werden. So hat der EDSA auch in seiner Stellungnahme[5] zu „Consent or Pay“-Modellen großer sozialer Online-Plattformen betont, dass personenbezogene Daten kein Handelsgut sind und die Ausübung des Datenschutzgrundrechts nicht zu einem kostenpflichtigen „Feature“ eines Dienstes werden darf. Verantwortliche müssen dies berücksichtigen, wenn sie prüfen, ob überhaupt ein „Consent or Pay“-Modell für ihren Dienst angemessen ist und wenn ja, welche Gebühr angemessen ist. Datenschutzbehörden können den Einfluss einer solchen Gebühr auf die Entscheidungsfreiheit

[5] EDSA Opinion 08/2024 – on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms, https://www.edpb.europa.eu/system/files/2024-04/edpb_opinion_202408_consentorpay_en.pdf

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

der betroffenen Person und die damit verbundene Wirksamkeit einer Einwilligung in die Datenverarbeitung zum Zweck verhaltensbezogener Werbung prüfen.

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