

„Innovative Datenpolitik: Potenziale und Herausforderungen“

**Schriftliche Stellungnahme von Rebekka Weiß, Senior Manager Government Affairs,
Microsoft Deutschland GmbH zur öffentlichen Anhörung des Ausschusses für Digitales
des Deutschen Bundestags am Mittwoch, 26. Juni 2024**

Vorbemerkungen

Die EU hat in den vergangenen zwei Legislaturperioden zahlreiche Rechtsakte erlassen, die die Datenpolitik berühren und damit einen umfassenden Regulierungsrahmen für Datenverarbeitung, Datensicherheit, Dateninfrastrukturen, Datenzugang und -austausch geschaffen.

Die Datenschutzgrundverordnung (DS-GVO) war dabei lange Dreh- und Angelpunkt der datenpolitischen Debatte. Dies hat den Diskurs stark geprägt und den Datenschutz fest in allen Unternehmen verankert. Es hat die datenpolitische Debatte aber zT auch auf datenschutzrelevante Fragestellungen verknüpft UND Bereiche der Datenökonomie bisher daher unterbelichtet gelassen – diese Aspekte müssen daher nun viel stärker in den Mittelpunkt gerückt werden, um einerseits die verschiedenen Regulierungsinstrumente einzubeziehen und andererseits eine neue Balance und einen ausgewogenen Interessensausgleich zu ermöglichen.

Es ist daher ausdrücklich zu begrüßen, dass die Anhörung zum Thema „Innovative Datenpolitik“ vor allem auch den EU Data Act (DA), den EU Data Governance Act (DGA), den EU Digital Services Act (DSA) und den EU AI Act sowie Fragen der Infrastrukturebene direkt in Bezug nimmt. Damit ist ein wichtiger Schritt getan und das Narrativ für eine innovativere Datenpolitik geöffnet.

Wir befinden uns zudem im Zeitalter der Künstlichen Intelligenz. Zukunfts- und innovationsoffene Entwicklung und Interpretation von Regulierungen wird entscheidend dafür sein, dass wir die Potenziale einer wirklich innovativen Datenpolitik so nutzen können, dass Politik, Unternehmen und die Gesellschaft vom enormen Potenzial der KI nachhaltig profitieren können.

Der nationale Gesetzgeber muss sich zeitnah zudem mit der Ausgestaltung der nationalen Aufsichtsstrukturen befassen. Benötigt wird ein sowohl nach innen (innerhalb Deutschlands bezüglich der beaufsichtigten Stellen) als auch nach außen (Abstimmung und Harmonisierung innerhalb der EU und international) funktionierendes System. Klare Zuständigkeitszuweisungen helfen dabei, den Unternehmen Sicherheit zu vermitteln, wer die richtigen Ansprechpartner sind. Nicht (nur) für Aufsicht und Kontrolle, sondern vor allem auch für Beratung und die gemeinsame Entwicklung von Interpretationen der verschiedenen Regulierungsinstrumente und ihres

Zusammenspiels. Keine einzelne Behörde wird dabei alle notwendigen Kompetenzen und die notwendige rechtliche und technische Expertise allein abdecken können – es wird auf Kooperation und Abstimmungen und die Einbeziehung von Fachbehörden und Experten aus der Praxis ankommen. Eine Bündelung dieser Koordinierungsfunktion bei der Bundesnetzagentur (BNetzA) als zuständige Aufsicht für DSA, DGA, DA und AI Act scheint der sinnvollste Weg zu sein, um Klarheit, Rechtssicherheit und Entscheidungsfähigkeit sicherzustellen.

Ein weiterer wichtiger Baustein für innovative Datenpolitik sind verstärkte (Förder-)Maßnahmen im Bereich der Standardisierung sowie der Entwicklung von (branchenspezifischen) Codes of Conducts bzw. Codes of Practices, die die Umsetzung und Implementierung der zahlreichen und verzahnten Regulierungen erleichtern. Hier sollten Politik, Wissenschaft und Unternehmen in den Entwicklungsgremien zusammenwirken, um praktikable, internationale anschlussfähige und für die Unternehmen umsetzbare Lösungen zu entwickeln.

Die nachfolgende Stellungnahme führt hierzu einige Details aus und bezieht sich auf den Fragenkatalog vom 7. Juni 2024, der insgesamt 18 Fragen umfasst.

Berlin, den 24. Juni 2024

Fragenkatalog und Antworten:

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?

Für eine innovative Datenpolitik ist angesichts der bereits bestehenden umfassenden Regulierung vor allem eine moderne, sichere und vertrauenswürdige Infrastruktur notwendig, die datengetriebene Geschäftsmodelle und Künstliche Intelligenz befähigt sowie Datenaustausch zwischen Industriepartnern und öffentlicher Hand ermöglicht.

Der Rechtsrahmen aus Data Governance Act und Data Act hat zahlreiche Möglichkeiten geschaffen, den Datenaustausch zu befördern.

Der deutsche Gesetzgeber sollte sich nun bei der Umsetzung weniger auf zusätzliche regulierende Vorschriften und stärker auf die Schaffung einer leistungsfähigen Dateninfrastruktur und die Förderung der digitalen Kompetenz fokussieren. Investitionsoffenheit und ein stabiler Rechtsrahmen sowie das klare Signal an Industrie und Wissenschaft, dass Dateninnovationen gefördert werden, sind dafür essentiell.

Die Bündelung der Aufsicht für digitalpolitische Dossiers sollte mit der Benennung einer zuständigen Stelle beginnen. Die BNetzA scheint hierfür geeignet und hat bezüglich der notwendigen Abstimmungsprozesse mit weiteren einzubeziehenden Behörden wichtige Vorerfahrungen. Zudem erfüllt sie bereits die Rolle als Digital Services Coordinator, was sich gut mit der Rolle der Daten- und KI-Aufsicht verzahnen lässt. Für Abstimmungsprozesse mit Datenschutzaufsichtsbehörden und sektoral zuständigen Aufsichtsbehörden wie Bafin, KBA oder auch dem BSI für Fragen der Informationssicherheit kann die BNetzA Anleihen an die Abstimmungsprozesse aus ihrer Rolle als DSC ziehen.

Eine Bündelung der Zuständigkeit muss dabei vor allem drei wesentliche Zwecke erfüllen:

- Klarheit für beaufsichtigten Unternehmen, wer zuständige Behörde und Ansprechpartner ist
- Sektor-, Rechts- und Technologieexpertise anderer Behörden in den Bewertungsprozess einbeziehen
- einheitliche Bewertungen inländischer Sachverhalte herbeiführen und Entwicklung als zentrale Stelle für europäische Abstimmungsprozesse

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?

Die zentralen Elemente einer innovativen, modernen, sicheren und vertrauenswürdigen Infrastruktur für eine innovative Datenpolitik umfassen die den Ausbau von Rechenzentren, Cloud-Technologie, IT-Sicherheitsstandards und Datenschutz. Eine ausgebauten Rechenzentren- und Cloudinfrastruktur ist von besonderer Bedeutung, da sie die Grundlage für effiziente und moderne Organisation von Unternehmen und Geschäftsmodellen und einer modernen Verwaltung bildet.

Innovative Datenpolitik basiert auf der Möglichkeit des dezentralen Arbeitens, flexibler Skalierungsfähigkeit und Vernetzung sowie Datenauswertungen mittels Methoden der Künstlichen Intelligenz. Die Cloud ist dafür faktisch und praktisch der sinnvollste Distributionskanal für IT-Services und KI – und damit auch für datengetriebene Verwaltung und Politikgestaltung.

Um insbesondere die öffentliche Verwaltung zukunftsfest und innovativ zu gestalten, bedarf es einer umfassenden Cloudifizierung der öffentlichen Verwaltung. Souveränitätsüberlegungen spielen hierbei eine wichtige Rolle. Souveränität muss dabei zum einen als mehrdimensionale und zum anderen als gestufte Anforderung verstanden werden, um Anforderungen gerecht zu werden und Skalierbarkeit sicherzustellen. Konkret heißt das:

- Nicht alle Cloud-Workloads sind gleich sensibel, daher ist es wichtig zu definieren, welcher Souveränitäts- und Sicherheitsgrad für welche Art von Workloads erforderlich ist.
- Ein entsprechender Rahmen für die Bewertung bieten die Cloud Platform Requirements des BSI, der einen Rahmen bis in hoch sensible Inhalte definiert.
- Souveränität, ob mit Blick auf Cloud- oder Datennutzung, muss in klare technisch implementierbare Vorgaben übersetzt werden. Dies ermöglicht die Gestaltung entsprechender Geschäftsmodelle und Angebote für alle Marktteilnehmer.

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?

Datenschutz ist integraler Bestandteil einer innovativen Datenpolitik. Datenschutz und innovative Datenpolitik sollten daher nicht als Gegensätze betrachtet werden, sondern als komplementäre Elemente, die gemeinsam einen Rahmen für verantwortungsvolle Innovation schaffen. Akzeptanz und Vertrauen in digitale Innovationen hängen dabei sowohl vom Datenschutz als auch von Praktikabilität und Nutzerfreundlichkeit der Dienste ab.

Es ist unerlässlich, eine Balance zwischen Datenschutz und Datennutzung zu finden. Dies erfordert ein chancenorientiertes Narrativ, das die Vorteile der Datennutzung hervorhebt, ohne die Bedeutung des Datenschutzes zu mindern. Der Reflex, bei jeder Innovation zuerst zu hinterfragen, ob diese Datenschutzvorgaben einhält, ist einer innovativen Datenkultur abträglich.

Die Abwägung von Interessen erfordert zudem vor allem Kenntnis über und Berücksichtigung von Rechtsgütern auch außerhalb des Datenschutzes. Dies gilt insbesondere im Kontext neuer technologischer Entwicklungen, die gesamtgesellschaftliche Mehrwerte bringen. Beispielhaft seien folgende Szenarien gebildet: Wenn wir beispielsweise dem Fachkräftemangel mit effizienzsteigernden KI-Anwendungen begegnen wollen, muss dieser Mehrwert auch bei der Datennutzung berücksichtigt werden. Bei der Erhebung und Nutzung von Trainingsdaten für die Weiterentwicklung des autonomen Fahrens müssen selbstverständlich auch ausreichend Datensätze aller Altersgruppen sowie von Menschen mit besonderen Mobilitätsanforderungen einbezogen werden können. Die Sicherheit aller Straßenverkehrsteilnehmenden und die Sicherheitsgewinne durch Fahrassistenzsysteme und autonomes Fahren müssen in eine Balance zu den Datenschutzinteressen gebracht werden. Gleiches gilt für Innovationen im Bereich des Gesundheitswesens, sowohl mit Blick auf Fortschritte in der Forschung als auch in der Digitalisierung des Gesundheitswesens als Ganzes. Nicht ohne Grund hat bereits das Gutachten der Datenethikkommission 2019 festgehalten, dass nicht nur die Nutzung sondern auch die Nichtnutzung von Daten ethisch zu verantworten ist.¹

Eine der jeweiligen Anwendung und Datennutzung angemessene Datensicherheit und Privacy Enhancing Technologies (PETs) werden in der Praxis bereits zur Anwendung gebracht (siehe hierzu auch Frage 16). Datentreuhandmodelle bzw. Datenplattformen für Datenräume können ebenfalls zum

¹ [BMI - Publikationen - Gutachten der Datenethikkommission \(bund.de\)](https://www.bmi.bund.de/SharedDocs/Gutachten/DE/2019/01/20190101-Datenethikkommission.html).

Einsatz gebracht werden – sie müssen jedoch skalierbar, international anschlussfähig und praktikabel ausgestaltet sein, um insbesondere Unternehmen dabei zu unterstützen Daten zu teilen. Es ist zu begrüßen, dass diesbezüglich auch verschiedentlich Forschungsprojekte gefördert werden, um branchenbezogene Lösungen zu finden.

Insbesondere falsch verstandener Datenschutz hat in der Vergangenheit dennoch zu viel Verunsicherung geführt. Eine innovative Datenpolitik muss hier ansetzen, ein neues Narrativ etablieren und der Komplexitäten von Dateninnovationen Rechnung tragen. Auch den Datenschutzaufsichtsbehörden kommt hier eine wichtige Rolle zu. Die Entwicklung einer harmonisierteren Auslegung der Datenschutzregeln und die Leistung eines Beitrags zu einer chancenorientierten Datenpolitik liegt auch in ihrer Hand. Dies gilt umso mehr, weil die Datenschutzaufsichtsbehörden, ganz unabhängig von der Strukturfrage, zukünftig auch in die Auslegung von Vorschriften vieler weiterer „Digitalgesetze“ einbezogen werden müssen.

In den vergangenen Jahren hat die Vielstimmigkeit im Datenschutzdiskurs in Deutschland teilweise dazu geführt, dass Dateninnovationen mit Skepsis begegnet wird und das Risikonarrativ das Chancennarrativ überlagert. Dies hat dazu geführt, dass innovative Geschäftsmodelle verzögert oder auch gar nicht durchgeführt wurden.² Es ist an der Zeit, diesen Trend umzukehren und einen positiven Diskurs über Dateninnovation zu fördern. Das beginnt auch bei der Digitalisierung der Politik selbst, die eine Vorreiterstellung bei der Nutzung innovativer Dienste einnehmen sollte. Daneben ist es Aufgabe der Unternehmen, innovative Datenprodukte und -services zu entwickeln, die für KundInnen und Partnerunternehmen attraktiv, skalierbar und nutzerfreundlich sind. Zusätzlicher Wettbewerb entsteht so auch durch den Aufbau lokaler Ressourcen, der innovative Geschäftsmodelle voranbringt, durch zusätzliche Absicherungen im Bereich der internationalen Datentransfers nach den Regeln der DS-GVO³ oder die Weiterentwicklung von Privacy Enhancing Technologies (PETs)⁴.

² [Fünf Jahre DS-GVO: Unternehmen sind weiterhin verunsichert | Presseinformation | Bitkom e. V.](#)

³ [Microsoft announces the phased rollout of the EU Data Boundary for the Microsoft Cloud begins January 1, 2023 - EU Policy Blog](#)

⁴ Siehe hierzu vor allem auch Frage 16.

4) Welche Elemente fehlen in Deutschland auf dem Weg zu innovativer Datenpolitik, wie können weitere Anreize für das Teilen von Daten in wechselseitigem Interesse weiter ausgebaut werden und welche Bedeutung – Stichwort Open Data, Datenlabore und Transparenzgesetz – kommen dem Staat und der öffentlichen Verwaltung zu und werden diese dieser gerecht?

Datenlabore und der Austausch zwischen den verschiedenen Stellen der öffentlichen Hand können wichtige Bausteine für eine innovative Datenpolitik sein. Die Finanzierung solcher Ansätze sollte sowohl auf Bundes- als auch auf Landes- und Kommunalebene sichergestellt sein. Innovative Datenpolitik darf nicht als Projekt einer Legislatur verstanden werden, sondern benötigt eine dauerhafte Struktur (und Finanzierung). Nur durch die Beständigkeit entsprechender Strukturen kann der notwendige Kulturwandel, der Kompetenzaufbau und die notwendige Data Literacy aller Verwaltungsangestellter dauerhaft in der öffentlichen Hand umgesetzt werden.

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?

Es gibt sowohl auf nationaler als auch auf EU-Ebene Ansätze, um den Datenzugang zu gewährleisten. Neben den Regelungen des DSA bieten beispielsweise auch der Data Act, das geplante Forschungsdatengesetz und Vorschriften im Gesundheitsbereich Hebel, um einen Datenzugang zu ermöglichen. Weiterer Regulierungen bedarf es daneben nicht zwangsläufig. Bessere und passgenauere Lösungen können stattdessen Codes of Conduct bieten.

Zudem haben kürzliche Fälle mit Empfehlungen der Kommission gezeigt, dass Datenzugänge auch neben gesetzlichen Verpflichtungen gewährt werden. Kooperative Ansätze, die es Unternehmen ermöglichen Datenzugänge unter Berücksichtigung ihrer eigenen Geschäftsinteressen und auch der Interessen ihrer KundInnen und NutzerInnen einzurichten, sollten daher gefördert werden. Über solche Lösungen kann anlassbezogen und ausgerichtet am Forschungsinteresse unter Mitwirkung der Unternehmen eine Balance zwischen Innovation, Forschungs- aber auch Datenschutzinteressen sowie Investitionsschutz und Geschäftsgeheimnisschutz gefunden werden.

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?

Um eine breite Nutzung von Daten und eine innovative Datenpolitik zu fördern, braucht es vor allem eine skalierbare Infrastruktur und die Förderung des digitalen Skillsets in der gesamten Bevölkerung. Ob in schulischen oder weiterführenden Bildungszweigen oder auch in beruflicher Fortbildung: Data Literacy, Medien- und Digitalkompetenz sowie Cybersecurity Trainings sind die wichtigen Bausteine für innovative Datenpolitik. Hier kann und sollte die Politik auf allen Ebenen Unterstützung und Finanzierung bewerkstelligen und Partnerschaften knüpfen, um den wachsenden Fortbildungsbedarf zu decken.⁵

Durch Kooperationen zwischen Schulungsdienstleistern, Instituten, Universitäten, gemeinnützigen Organisationen und Unternehmen können Ansätze skaliert werden, sodass die gesamte Gesellschaft erreicht wird.

Beispielhaft sei die Initiative „IT-Fitness“ erwähnt, die Microsoft gemeinsam mit dem Förderverein für Jugend und Sozialarbeit e.V. (fjs) entwickelt hat. Diese bieten beispielsweise kostenlose und einsteigerfreundliche Lernerfahrungen in den Bereichen KI, Cybersecurity und Green Digital Skills in Deutschland an – mit dem Ziel, mehr als 550.000 Menschen zu erreichen. Auch die Initiative „BoostYourSkills“ ist aus einer Industriepartnerschaft in Zusammenarbeit mit Unternehmen wie Schaeffler und DHL Group entstanden. Sie ist auf einen erfolgreichen Berufseinstieg ausgerichtet und soll einen Karrierestart in Bereichen erleichtern, in dem digitale Fähigkeiten immer wichtiger werden. Auch die ReDI School of Digital Integration stellt digitale Skills in den Mittelpunkt: Sie hilft geflüchteten Menschen und marginalisierten Gruppen, einen Arbeitsplatz in der deutschen IT-Branche zu finden.

Jede politische Einheit, jede Verwaltungsstelle (und auch jede Organisation aus Wissenschaft und Unternehmen) sollte in der Zeitplanung ihrer Mitarbeitenden ein Stundenkontingent einplanen, das dezidiert für den Aufbau dieser neuen Kompetenzen verwendet werden kann.

⁵ Auch gesetzlich bestehen zukünftig Anforderungen an Training und Schulungen für Mitarbeitende. So sieht beispielsweise Art. 4 AI Act („KI-Kenntnisse“) vor, dass Anbieter und Betreiber von KI-Systemen Maßnahmen ergreifen müssen, damit ihr Personal (und Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind) über ausreichende KI-Kenntnisse verfügen.

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

8) Welche Möglichkeiten gibt es, mithilfe von datenbasierten Anwendungen der Klimakrise zu begegnen und welche datenpolitischen Maßnahmen sind notwendig, um das Potential für eine nachhaltige Digitalisierung sowie für einen innovativen Klimaschutz voll auszuschöpfen?

Umweltschutz und Nachhaltigkeit sind von zentraler Bedeutung für Unternehmen und Politik. Datenbasierte Prognosen können und müssen dafür eingesetzt werden, um die bevorstehenden Herausforderungen konkret abschätzen zu können. So können wir auf der Grundlage von Daten Antwortstrategien entwickeln und bewerten. Datengetriebene Technologien und Künstliche Intelligenz sind daher zweifellos Teil der Lösung.⁶ KI ist dabei nicht die Lösung an sich, sondern ein entscheidendes Werkzeug, das Wissenschaftler, Forscher, Unternehmen und die Politik nutzen können, um präziser zu arbeiten und effizienter mit maßgeschneiderten Methoden reagieren zu können.

KI kann zudem dazu beitragen, nachhaltige Energie zu fördern und den Klimawandel zu bekämpfen. Beispielsweise kann sie den Menschen dabei helfen, ihren Energieverbrauch zu optimieren, das Energieangebot und die Nachfrage besser vorherzusagen und darauf zu reagieren. Neue Analysen können zudem Wetterextreme genauer vorhersagen oder auch die Wiederaufforstung beschleunigen, indem sie die besten Gebiete für die Bepflanzung ermittelt. Zugleich muss selbstverständlich daran gearbeitet werden, moderne Technologien so energiesparsam und nachhaltig wie möglich zu gestalten.

Die Wettbewerbsfähigkeit in Deutschland wird jedoch bisher zum Teil durch hohe Energiekosten, Fachkräftemangel und aufwändige bürokratische Genehmigungsprozesse beeinträchtigt. Jedoch zeigen aktuelle Projekte, dass die Verzahnung von Nachhaltigkeit, Nutzung regenerativer Energien und Ansiedlung innovativer Datenstrukturen möglich ist.⁷ Innovative Datenpolitik und der Einsatz von modernen Technologien zur Bekämpfung des Klimawandels muss daher auch die Bedeutung von Rechenzentren in den Mittelpunkt stellen.

⁶ Zu den CO₂-Einsparmöglichkeiten durch digitale Technologien siehe [Klimaeffekte der Digitalisierung 2.0 | Studie 2024 | Bitkom e. V.](#)

⁷ [Machbarkeitsstudie: Das Rheinische Revier eignet sich hervorragend als Drehkreuz für den Austausch, die Speicherung und die Nutzung großer Datenmengen | Wirtschaft NRW](#)

9) Wie beurteilen Sie das Zusammenwirken der zahlreichen Dateninitiativen (z.B. Dateninstitut, MISSION KI, Gaia-X Hub, Förderprojekte, Datenraumvereine, Data Spaces Support Center, Gaia-X etc.) auf deutscher und europäischer Ebene im Hinblick auf Ihre Kohärenz und Zielerfüllung? Wie bewerten Sie ihr Einzahlen auf die Erfüllung von Compliance-Pflichten durch die Wirtschaft, das Ausnutzen von unternehmerischen Effizienzreserven und der Schaffung von Schlüsselinnovationen in Europa, die das Potential haben, ganz neue Märkte zu schaffen?

Grundsätzlich ist zu begrüßen, dass in verschiedenen Projekten und Initiativen Schlüsselfragen der Datenökonomie analysiert und bearbeitet werden. Forschungsprojekte z.B. im Bereich der Datenräume sind wichtige Ergänzungen, um vor allem zukunftsfähige Datennutzungen zu erarbeiten.

Die Verzahnung der einzelnen Initiativen untereinander und auch die inhaltliche Verzahnung bzw. inhaltliche Erweiterung zwischen Datennutzung und KI sind jedoch ausbaufähig. Die Zielerfüllung aller Initiativen muss sich in jedem Fall an ihrer Praktikabilität messen lassen. Die Nutzbarkeit der Ergebnisse hängt dabei unter anderem davon ab, wie gut die Einbeziehung der Praxis im Entwicklungsprozess umgesetzt wird. Aufgrund der Vielzahl an Initiativen ist es jedoch für viele Unternehmen aus Kapazitätsgründen kaum möglich, sich einzubringen. Zudem wird in den verschiedenen Projekten, Instituten und Förderprogrammen häufig parallel an ähnlichen Fragen gearbeitet. Die Dopplung führt zu zusätzlichen Aufwänden. Bei der Evaluierung der Projekte sollte daher auch eine Zusammenlegung und vor allem der Anschluss an internationale Dateninitiativen und -projekte erwogen werden.

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?

Die 2023 veröffentlichte Datenstrategie betont grundsätzlich die richtigen Zielstellungen: die Nutzung und Verwaltung von Daten, um Innovationen und Fortschritt zu fördern. Positiv ist außerdem die klare Betonung der Bedeutung einer neuer Datenkultur.

Die bisherige Umsetzung der Strategie zeigt Fortschritte, jedoch bleibt entscheidend, dass klare Aufträge und Umsetzungszeiträume festgelegt werden, um die Effektivität und Transparenz der Maßnahmen zu gewährleisten. Dies war bereits eine Stärke der früheren Datenstrategie und sollte beibehalten werden. Zudem sollten Priorisierungen klar definiert und in die Strategie eingearbeitet werden, um sicherzustellen, dass die wichtigsten Maßnahmen zuerst umgesetzt werden.

Zudem ist es von großer Bedeutung, dass die Datenstrategie von einer chancenorientierten Kommunikationsstrategie flankiert wird. Eine solche Strategie sollte die Vorteile der Datennutzung hervorheben und dabei vor allem bei innovativen Datennutzungsmodellen der öffentlichen Hand auf die Fragen von Bürgerinnen und Bürger eingehen. Investitionen in die digitale Infrastruktur und die Schaffung von Rechtssicherheit für Unternehmen sind ebenfalls wichtige Bestandteile, um die Zukunftsfähigkeit der deutschen Datenpolitik zu sichern. Diese Bausteine sollten in der Datenstrategie zukünftig noch stärker hervorgehoben werden.

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?

Für eine innovative Datenpolitik in Deutschland ist weniger die Struktur der Datenschutzaufsicht allein entscheidend, als eine zukunftsorientierte Einbeziehung von verschiedenen Behörden für die Auslegung und Umsetzung des gesamten digitalpolitischen Regelungsrahmens. Datenverfügbarkeit und -nutzbarkeit sind angesichts der Vielzahl an neuen Regulierungsinstrumenten und auch der technologischen Entwicklung keine Fragen mehr, die sich nur nach Datenschutzrecht entscheiden lässt.

Die DS-GVO wird durch zahlreiche datenrechtliche Regulierungsinstrumente (insb. Data Act, Data Governance Act, AI Act, EHDS) und digitale Rechtsakte (bspw. Digital Services Act, Digital Markets Act) ergänzt, die allesamt datenbezogene Regelungen und Rechte enthalten.

Die Weiterentwicklung der deutschen Aufsichtslandschaft muss daher umfangreicher angegangen und funktionierende Konsultationsmechanismen entwickelt werden. Eine wichtige Weichenstellung kann dabei dadurch erreicht werden, dass die Aufsicht in Aufstellung, Funktionsweise und Finanzierung so ausgestattet wird, dass Kapazitäten für Beratung und Begleitung innovativer Datenprojekte frei sind. Die Aufsichts Bündelung bei der BNetzA kann eine wichtige Weichenstellung für eine zukunftsfähige Aufsichtsstruktur sein. Dies würde auch den Wechsel von Risiko- zum Chancennarrativ nachhaltig fördern und den beaufsichtigten Unternehmen die benötigte Rechtssicherheit geben.

Eine grundlegende Reform der DS-GVO selbst braucht es für eine innovative Datenpolitik zum jetzigen Zeitpunkt nicht. Um konkrete Datennutzungen zukünftig zu erleichtern, scheint es eher angezeigt, neue Erlaubnistatbestände in EU-Verordnungen zu etablieren. Die Evaluierung der EU-Kommission zur Frage der DS-GVO Reform hat ebenfalls bestätigt, dass die europäische Industrie wenig Vorteile in einer Überarbeitung der DS-GVO sieht. Die Gründe hierfür sind vielfältig: die voraussichtlich lange Zeit und der Aufwand für die Überarbeitung, Investitionsschutz für getätigte Umsetzungs- und

Compliancestrecken, erlangtes Vertrauen durch den derzeitigen Rechtsrahmen und ein insgesamt hoher Implementierungsaufwand durch die Vielzahl an Regulierungen.

Zudem sind die neueren Digitalrechtsakte alle mit der DS-GVO verzahnt und arbeiten mit Pauschalverweisen auf deren Geltung. Eine nun erfolgende Änderung der DS-GVO könnte daher neue Fragen auch hinsichtlich der weiteren datenbezogenen Rechtsakte aufwerfen und die Rechtssicherheit für Unternehmen eher senken als erhöhen.

Zwar sind größere Änderungen an der DS-GVO im Moment nicht notwendig, doch könnten der EDSA und die Datenschutzbehörden der Mitgliedstaaten in wichtigen Bereichen neue Leitlinien bereitstellen, die die Verbraucher schützen, die Sicherheit für Unternehmen erhöhen und die neuen Rechtsakte sowie technologische Entwicklungen mit berücksichtigen. In den vergangenen Jahren hat sich der Datenschutzdiskurs allzu häufig auf die Einwilligung als Rechtsgrundlage der Datenverarbeitung fokussiert. Die Gleichrangigkeit der verschiedenen Erlaubnistatbestände und insb. die Bedeutung der Datenverarbeitung nach Art. 6 Abs. 1 lit. f DS-GVO (berechtigtes Interesse) für die Datenökonomie könnten in einer aktualisierten Leitlinie der Aufsicht betont werden. Daneben wäre die Aktualisierung der Leitlinien der Artikel-29-Arbeitsgruppe aus dem Jahr 2014 zur Verwendung anonymer und pseudonymer Daten angezeigt. Letzteres wäre besonders wichtig, um die Entwicklung neuer Technologien, einschließlich (generativer) KI, zu unterstützen.⁸

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?

Die Umsetzung des Data Act und des AI Act kann durch Standardisierungsarbeiten, Codes of Conduct und Codes of Practices in mehrfacher Hinsicht erleichtert werden. Diese Instrumente können dazu beitragen, klare und einheitliche Rahmenbedingungen zu schaffen, die sowohl die Entwicklung als auch die Anwendung von KI-Technologien fördern und gleichzeitig Transparenz und Kontrolle über Daten gewährleisten. Insbesondere die Arbeit in internationalen Standardisierungsgremien ist hier von essentieller Bedeutung, da sie die Anschlussfähigkeit der Lösungen und Rechtssicherheit auch bei übergreifenden Geschäftsmodellen sicherstellt. Es ist zu begrüßen, dass bereits Standardisierungsvorhaben durch die EU Kommission an das Joint Technical Committee bei CEN/CENELEC (JTC21)⁹ gegeben wurden, die Transparenz, Sicherheit, Robustheit uvm. in den Bearbeitungsmittelpunkt rücken und die Konformitätsbewertung unter dem AI Act erleichtern werden.

⁸ Zu Anonymisierung siehe auch Frage 14, sowie zu PETs Frage 16.

⁹ [Artificial Intelligence - CEN-CENELEC \(cencenelec.eu\)](https://www.cenelec.eu/)

Bestehende Standards, wie ISO 42001 und ISO 23894 können und sollten zudem nutzbar gemacht werden für den AI Act, da diese sowohl Interoperabilität als auch Qualitätssicherung und Risikobewertungen in den Mittelpunkt stellen. Dies sind Bewertungsaspekte, die auch für den AI Act zentral sind. Damit werden wichtige Fragen adressiert, die alle Unternehmen bei der Umsetzung des AI Acts beantworten (können) müssen.¹⁰

Daneben sind Codes of Practices ein weiterer Baustein für praxistaugliche Umsetzung der Verpflichtungen, insbesondere mit Blick auf Transparenzvorgaben. Diese sind auch ausdrücklich vom AI Act vorgesehen.¹¹

Aus den Erfahrungen mit Codes of Conduct unter der DS-GVO können wichtige Lehren gezogen werden und etablierte Mechanismen zur Erarbeitung und zum Monitoring fortgesetzt bzw. an diese angeknüpft werden. Für Schnittstellenbereiche zwischen DS-GVO und Data Act könnten CoCs vor allem bei Fragen zu technischen Maßnahmen, Rollen der Datennutzenden und Kontrolle über die verarbeiteten Daten wichtige Ergänzungen bieten und die Umsetzung erleichtern. Der auf CoC Ebene geführte praxisnahe Dialog und Austausch innerhalb von Sektoren und Industriebereichen erleichtert den beteiligten Unternehmen und Organisationen die Umsetzung und leistet einen wichtigen Beitrag zu Etablierung von Industriestandards. Auch in diesem Zusammenhang sind die sachgerechte Ausstattung und Ausgestaltung der Aufsicht entscheidend. Bisherige CoC Erarbeitungen im Bereich der DS-GVO haben (leider) gezeigt, dass die Genehmigungen zu langwierig sind und zT an Zuständigkeitsstreitigkeiten zwischen den Aufsichten in Europa scheitert.

Dennoch bieten alle Instrumente (Standardisierung, CoCs und CoPs) wichtige Potenziale für die Umsetzung der Rechtsakte.

Zusammenfassend können diese Instrumente dazu beitragen, die rechtlichen Anforderungen des Data Act und des AI Act zu operationalisieren und somit ihre Umsetzung zu erleichtern. Sie können auch die Akzeptanz von KI-Technologien erhöhen, indem sie Vertrauen schaffen und sicherstellen, dass KI im Einklang mit gesellschaftlichen Werten und Normen entwickelt und eingesetzt wird.

Die Bedeutung von internationalen Standards ist dabei für die Umsetzung des EU AI Act von großer Relevanz. Internationale Standards können dazu beitragen, die Anforderungen des AI Act zu harmonisieren und die Einhaltung zu erleichtern, indem sie klare Richtlinien für die Entwicklung und den Einsatz von KI-Systemen bieten. Sie fördern die Interoperabilität und Kompatibilität von KI-

¹⁰ Es sind bereits verschiedene Standards im Bereich Künstliche Intelligenz auf internationaler Ebene entwickelt worden, die nun nutzbar gemacht werden können und sollten: ISO 38507 (Governance of IT – Governance Implications of the use of artificial intelligence by organizations), ISO 23894 (Risk Management); ISO 42005 (System Impact Assessment Guidance); ISO 42006 (Certification Body requirements); ISO 42001 (Artificial Intelligence Management system).

¹¹ Art. 56 AI Act.

Systemen über Grenzen hinweg und unterstützen somit die Schaffung eines einheitlichen Marktes für KI-Produkte und -Dienstleistungen innerhalb der EU.

13) Welche Maßnahmen sind aus Ihrer Sicht prioritär, um eine starke Datenökonomie und ein innovatives Daten-Ökosystem mit Rechen- und Datenzentren in Deutschland und Europa aufzubauen und die Ansiedlung von Daten-getriebenen Unternehmen zu erleichtern?

Die Schaffung einer modernen Rechenzentren-Infrastruktur ist für ein innovatives Daten-Ökosystem unerlässlich. Vor allem Hyperscale-Rechenzentren¹² sind wichtige Säulen für eine sich schnell entwickelnde Datenwirtschaft.

Für die Bereitstellung dieser Infrastruktur ist vor allem ein vorhersehbares und effizientes Genehmigungssystem für Rechenzentren wichtig.

Ein Beispiel aus Finnland zeigt, dass dort eine Gesetzgebung für "grüne Übergangprojekte" eingeführt wurde, die sich positiv auf viele Rechenzentrenprojekte auswirkt, die den grünen Wandel Finnlands unterstützen sollen und daher von einem beschleunigten Genehmigungsverfahren profitieren. Darüber hinaus ist die finnische Regierung dabei, einen "One-Stop-Shop"-Mechanismus einzuführen, um eine reibungslosere und schnellere Umweltgenehmigung zu fördern. Derartige Maßnahmen können ein entscheidender Wettbewerb für Märkte sein, die umweltfreundliche Investitionen und Arbeitsplätze anziehen und durch den Bau von Rechenzentren nachhaltige Standortvorteile für die Datenwirtschaft schaffen. Bei allen regulatorischen Maßnahmen, die sich auf den Bau von Rechenzentren auswirken oder direkt beziehen ist daneben vor allem wichtig, dass eine frühzeitige Information über entsprechende Gesetzesvorhaben erfolgt. Der Bau von Rechenzentren ist regelmäßig ein mehrere Jahre umspannender Planungs- und Aufbauprozess. Planungssicherheit und die Einbeziehung zukünftiger Anforderung bereits in der Planungsphase sind daher entscheidend, um Vorhersehbarkeit sicherzustellen.

Um eine starke Datenökonomie und ein innovatives Daten-Ökosystem mit Rechen- und Datenzentren in Deutschland und Europa aufzubauen und die Ansiedlung von datengetriebenen Unternehmen zu erleichtern, sind daher folgende Maßnahmen prioritär:

¹² Hyperscale-Rechenzentren zeichnen sich aus durch extreme Skalierbarkeit, Flexibilität in Bezug auf Rechen- und Speicherleistung, Ausrichtung auf Workloads in großem Umfang, optimierte Netzwerkinfrastruktur und -konnektivität bei zugleich minimaler Latenz. Darin liegen auch die besonderen Mehrwerte: So wie die Fahrt mit einem Hochgeschwindigkeitszug schneller und energieeffizienter ist als die Fahrt mit dem eigenen Auto, bietet die Nutzung der Möglichkeiten eines Hyperscale-Rechenzentrums eine bessere Energieeffizienz, mehr Sicherheit und innovative Dienste für die Daten von Unternehmen und Organisationen (im Vergleich zu einzelnen Rechenzentren vor Ort).

- Investitionen in digitale Infrastruktur: Der Aufbau und die Erweiterung von hochleistungsfähigen Rechenzentren und Dateninfrastrukturen sind grundlegend, um die Datenverarbeitung und -speicherung zu unterstützen. Dies beinhaltet auch die Förderung von Cloud-Infrastrukturen und Diensten, die eine sichere und effiziente Datenverarbeitung ermöglichen. Ein stabiles Investitionsklima und vorhersehbare Genehmigungsprozesse sind entscheidende Weichenstellungen.
- Rechtliche und technische Rahmenbedingungen: Es ist wichtig, rechtliche und technische "Brücken" zu schaffen, die sichere Datenkooperationen und Industriepartnerschaften, auch zur Entwicklung des KI-Ökosystems, ermöglichen. Die Entwicklung von internationalen Standards muss durch Industrieexperten und Politik priorisiert werden, um anschlussfähige Technologien voranzubringen. Ebenso sollten Labelling Schemes und Zertifizierungen auf europäischer Ebene entwickelt werden. Es ist zu begrüßen, dass beispielsweise bereits ein „Labelling Scheme for Data Center Sustainability“ auf europäischer Ebene angestoßen wurde. Solche europäischen und internationalen Zertifizierungen und Labels können eine wichtige Brücke bilden, da sie Vertrauen in die Dateninfrastruktur stärken und die Einhaltung der zahlreichen datenbezogene Regulierungsinstrumenten unterstützen.
- Förderung von Datenkompetenz: Aufbau von Fähigkeiten im Bereich der Datenkompetenz brauchen Förderung und Finanzierung.

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?

In der Praxis werden bereits seit vielen Jahren erfolgreich Anonymisierungsverfahren eingesetzt und Datenbestände angelegt, die personenbezogene und nicht-personenbezogene Daten zu separieren.

Rechtliche Unsicherheiten bzw. jahrelange Diskussionen in Deutschland über (z.T. rein theoretische) Re-Identifizierungs-Risiken haben indes zu Verunsicherungen geführt. Dabei haben erfolgreiche Anonymisierungsverfahren, die auch in Absprache mit den Aufsichtsbehörden entwickelt wurden, gezeigt, dass Unternehmen vor allem bei umfangreichen Datenauswertungsprozessen oder Datenkooperation auch mit anonymisierten Datensätzen arbeiten können und wollen.

Die Abgrenzung zwischen personenbezogenen und nicht-personenbezogenen Daten wird vor dem Hintergrund des EU Data Acts noch zusätzliche Bedeutung erlangen. Der EU Data Act erfasst sowohl personenbezogene als auch nicht personenbezogene Daten, lässt aber zugleich die DS-GVO

unberührt, sodass für die vom Data Act erfassten personenbezogenen Daten auch die DS-GVO mit allen Rechten und Verpflichtungen gilt.

Zukünftige Leitlinien in diesem Bereich sollten daher vor allem folgende Elemente beachten/beinhalten:

- Branchenunterschiede berücksichtigen
- Geänderte rechtliche Rahmenbedingungen einbeziehen (Anonymisierung ist kein alleiniges DS-GVO-Thema mehr)
- Risikobasierte Ansätze abbilden, die die Wahrscheinlichkeit einer Re-Identifizierung nach erfolgter Anonymisierung angemessen berücksichtigen
- Technische Standards (technikneutral und zukunftsorientiert) einbeziehen, um praktische Anleitungen zu geben, wie Anonymisierung erfolgreich durchgeführt werden kann und den Fokus auf Chancen und Potenziale zu lenken

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?

Rechtsunsicherheiten bei Fragen des internationalen Datentransfers wirken sich stets auf Innovationen und Geschäftsmodelle aus, die auf Transfers und internationale Kooperation ausgerichtet sind. Die Umsetzung der Vorgaben und ein datenschutzkonformer Datentransfer sind selbstverständlich möglich, aber in der Praxis natürlich mit Aufwänden und verschiedenen Risikoassessments verbunden.¹³ Rechtssicherheit und Verlässlichkeit von Transfermechanismen und auch internationalen Abkommen über Zugriffe auf Daten sind daher für Unternehmen entscheidend.

Das gilt umso mehr, da auch der EU Data Act in Kapitel VII Vorgaben zu Übermittlungen, Zugriffen und Transfers im internationalen Umfeld enthält und Kooperationen und Partnerschaften für die gemeinsame und Weiterentwicklung von KI-Services und -produkten in Zukunft zusätzliche internationale Kooperationen und internationalen Datentransfers erfordern wird.

Das für den EU-US Transfer im Juli erlassene Data Privacy Framework (DPF)¹⁴ bildet zur Zeit den relevanten Rahmen zur Absicherung des Transfers nach der DS-GVO und unterscheidet sich insofern

¹³ Beispielhaft sei diese praktische Hilfestellung für Unternehmen erwähnt: [Bitkom Transfer Impact Assessment Tool \(BiTIAT\) | Bitkom e. V.](#)

¹⁴ [Adequacy decision EU-US Data Privacy Framework_en.pdf \(europa.eu\)](#)

von seinen Vorgängerabkommen, dass die dem DPF vorangegangene Executive Order zusätzliche Mechanismen in das US-Rahmenwerk eingearbeitet hat.¹⁵ Auf z.T. geäußerte Bedenken hinsichtlich der zugrundeliegenden Executive Order und der Überprüfungsgerichte sei nachfolgend eingegangen.

Die Executive Order selbst entfaltet volle Gesetzeskraft und ist für die Executive verbindlich, einschließlich der US-Geheimdienste und Strafverfolgungsbehörden. Der Erlass ist nicht nur wirksam, sondern auch als dauerhafter Mechanismus anzusehen. Frühere Executive Orders, die sich auf nationale Sicherheit und Überwachung bezogen, erhielten parteienübergreifende Unterstützung und wurden auch von nachfolgenden Regierungen anerkannt.¹⁶ Und selbstverständlich ist die EU in der Lage, die dauerhafte Wirkung der Executive Order sicherzustellen, indem sie ihre Entscheidung über die Angemessenheit und den Fortbestand des DPF von der Existenz der Executive Order (oder von ähnlichen zukünftigen Bestimmungen) abhängig macht.

Der sogenannte Data Protection Review Court (DPRC) wird zum Teil als nicht unabhängig genug angesehen, weil er durch einen Exekutivakt eingerichtet wurde und nicht Teil der Gerichtsbarkeit nach Art. 47 der Charta und der US-Verfassung sei, sondern ein Gremium innerhalb der Exekutive der US-Regierung. Er sei daher keine ausreichende Verbesserung gegenüber dem früheren „Ombudsmann“-System unter dem Privacy Shield. Der Ombudsperson nach dem Privacy Shield fehlte jedoch die Unabhängigkeit bei der Ernennung, Überwachung und Abberufung der eingesetzten Entscheidungsträger. Das US-Justizministerium hat den DPRC nun durch entsprechende Verordnungen eingerichtet und operationalisiert. Der DPRC-Mechanismus garantiert, dass die Entscheidungsträger unabhängig sind, obwohl sie in der Exekutive untergebracht sind. Weder Generalstaatsanwalt noch andere Exekutivorgane dürfen die unabhängige Arbeitsweise des DPRC beeinflussen. Die vom DPRC erlassenen zukünftigen Entscheidungen in Beschwerdefällen sind zudem für alle US-Nachrichtendienste verbindlich, da dem DPRC die vollen Befugnisse eines Generalstaatsanwalts übertragen wurden.

Der Themenkomplex internationale Datentransfers ist insgesamt komplex und vielschichtig. So wie das Risiko von Datenverarbeitungen von verschiedenen Faktoren abhängt (und dies auch durch den risikobasierten Ansatz der DS-GVO gewürdigt wird), sind auch Risikoabwägungen bei internationalen Transfers notwendig. Verknäppte Darstellungen und Pauschalantworten (sämtliche Transfers sind unmöglich bzw. sämtliche Transfers in Drittstaaten sind unproblematisch) beschädigen das Vertrauen

¹⁵ Übersicht zum DPF: [Questions & Answers: EU-US Data Privacy Framework \(europa.eu\)](#) und hier [EU-US Data Privacy Framework \(europa.eu\)](#).

¹⁶ So wurde beispielsweise die PPD-28 der Obama-Regierung unverändert bis zur Verschärfung in der aktuellen Executive Order und wurde sowohl von der Trump-Administration als auch von der Biden-Administration fortgeführt. Noch langlebiger war Reagan's Executive Order 12333 aus dem Jahr 1981, die 40 Jahre wirkte und im Laufe der Jahre lediglich aktualisiert wurde.

in eine globale Datenwirtschaft in der Industriepartner und Partnernationen gemeinsame wirtschaftliche und gesellschaftliche Potenziale durch Datennutzung heben (wollen).

Im Spannungsfeld zwischen Datenschutz, Sicherheitsinteressen und unter Berücksichtigung verschiedener Risikokonstellationen, die von zahlreichen Faktoren wie verarbeiteten Daten, eingesetzten Datensicherheitstechnologien, dem tatsächlichen Zugriffsrisiko etc. abhängig sind, ist der größte Beitrag für Rechtssicherheit neben dem Bestand von internationalen Abkommen wie dem DPF und den weiteren erlassenen Adäquanzentscheidungen der EU Kommission ein faktenbasierter und lösungsorientierter Dialog - sowohl zwischen Politik, Zivilgesellschaft und Unternehmen.

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?

Besonderes Potenzial für Innovationen im Bereich des Datenschutzes bieten Entwicklungen von Privacy Enhancing Technologies (PETs). PETs umfassen verschiedene technische Ansätze wie z.B. Anonymisierungstechniken, die Entwicklung synthetischer Datensätze und K-Anonymität. Trotz der zunehmenden Anerkennung ihres Potenzials zur Erleichterung einer verantwortungsvollen und die Privatsphäre schützenden Datennutzung stehen PETs aus einer Reihe von Gründen weiterhin Hindernisse für eine breitere Akzeptanz entgegen:

- Der Bekanntheitsgrad von PETs ist nach wie vor begrenzt. Potenzielle Nutzer von PETs müssen weiter darüber aufgeklärt werden, was diese bewirken können, welche Möglichkeiten und Grenzen sie haben, welche Vorteile und Risiken sie bieten und wann sie eingesetzt werden sollten.
- Die Entwicklung und Umsetzung von PETs kann schwierig sein. Viele Technologien sind relativ neu und erfordern Fachwissen; nicht alle sind gleich gut entwickelt, und viele sind ressourcenintensiv, so dass ihre Einführung in manchen Fällen relativ teuer ist. Nicht immer sind ein hoher Reifegrad oder Standards vorhanden.
- Die politischen und rechtlichen Rahmenbedingungen für PETs sind noch weitgehend unentwickelt. Nur wenige Länder haben bisher regulatorische Vorgaben für PETs gemacht, geschweige denn deren Einsatz aktiv gefördert. Viele Regulierungsbehörden sind noch dabei, ihr Verständnis für diese Technologie zu entwickeln. In Fällen, in denen sich die Regulierungsbehörden nicht direkt mit diesen Technologien und ihrer Anwendbarkeit auf die Einhaltung von Rechtsvorschriften befasst haben, wird die Rechtsunsicherheit in Bezug auf die Einführung von Technologien zum Schutz der Privatsphäre eine Herausforderung bleiben und deren Potenzial daher nicht ausreichend genutzt.

Ein aktueller Vorschlag der Kommission für eine Verordnung über europäische Statistiken zu Bevölkerung und Wohnen¹⁷ zielt darauf ab, die Konsistenz aller auf Personen und Haushalten basierenden EU-Sozialstatistiken zu verbessern, indem die Rechtsgrundlage gestärkt und die Entwicklung innovativer Lösungen für den Datenaustausch zwischen den EU-Mitgliedstaaten gefördert wird. In Bezug auf "innovative Lösungen zur Ermöglichung des Datenaustauschs" bezieht sich der Vorschlag ausdrücklich auf PETs, um den Datenaustausch in Übereinstimmung mit den EU-Rechtsvorschriften zum Schutz personenbezogener Daten durchzuführen. Um eine wirksame gemeinsame Nutzung von Daten zu Qualitätszwecken im Einklang mit DS-GVO zu ermöglichen, fordert dieser Vorschlag die Erprobung und Nutzung von Technologien zur Verbesserung des Datenschutzes, die die Datenminimierung durch Technik umsetzen. Solche regulativ fördernden Mechanismen sollten ausgebaut werden, um die Entwicklung, den Einsatz und die Akzeptanz von PETs zu steigern.

Aufbauend auf solchen und ähnlichen vielversprechenden Initiativen sollten folgende Fördermaßnahmen ergriffen werden, um die weitere Entwicklung und Annahme von PETs voranzutreiben:

- Regulierungsbehörden und politische Entscheidungsträger sollten Anreize für die Verwendung von PETs schaffen. Um die Einführung von PETs zu fördern, sind klare regulatorische Vorgaben erforderlich. Die Unternehmen benötigen eine Anleitung, wie die Aufsichtsbehörden den Einsatz der Technologie zur Erfüllung gesetzlicher und behördlicher Verpflichtungen interpretieren und wie PETs bei Überlegungen zur Durchsetzung berücksichtigt werden. Wenn Regulierungs- und Durchsetzungsbehörden beispielsweise Parteien, die PETs einsetzen, Erleichterungen zur Verfügung stellen und die Verwendung von PETs als potenziell mildernde Faktoren in Betracht ziehen, sollten diese Erleichterung explizit in Leitlinien oder Verordnungen festgehalten werden. Die Regulierungsbehörden könnten ebenfalls klarstellen, ob die Nichtverwendung leicht verfügbarer PETs als potenziell erschwerender Faktor interpretiert wird.
- Entwickler und Anbieter von PETs, Forschungseinrichtungen, Aufsichtsbehörden und Regierungen sollten Maßnahmen ergreifen, um die Aufklärung zu PETs auszubauen.¹⁸ Um eine breite Akzeptanz zu erreichen, brauchen potenzielle Nutzer konkrete Nachweise und Erläuterungen zum Wert von PETs und dafür, wie sie zur verantwortungsvollen Datennutzung beitragen. Fallstudien über den Einsatz von Technologien sind zu diesem Zweck besonders zielführend.

¹⁷ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0031>.

¹⁸ Beispielhaft sei dieser Use Case für synthetische Datensätze und K-Anonymität erwähnt: [Dashboards und Datensätze | CTDC \(ctdatacollaborative.org\)](#)

- Durch Forschung, Experimentierräume und Diskussionen müssen die Beteiligten, darunter Regulierungsbehörden, Branchenexperten, Forscher und Datenschutzbeauftragte, Leitlinien und bewährte Verfahren für PETs entwickeln. Das Fehlen von Normen für PETs ist derzeit ein Hindernis für eine breitere Akzeptanz. Normen sind wichtig, um die Interoperabilität zu erleichtern, wenn verschiedene Technologien zum Schutz der Privatsphäre gemeinsam und länderübergreifend eingesetzt werden. Durch die Schaffung gemeinsamer Rahmenbedingungen können verschiedene PETs problemlos miteinander kommunizieren und zusammenarbeiten, indem Kompatibilität und Konsistenz hergestellt werden. Normen fördern auch das Vertrauen in diese Technologien, stellen sicher, dass PETs auf hohem technischen Niveau entwickelt werden, und fördern die Umsetzung, indem sie ein hohes Maß an Sicherheit bieten.

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 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?]

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

Mit dem EU Data Act wurde der Datenaustausch und die Datennutzung im wirtschaftlichen Austauschverhältnis EU-weit geregelt. Der Rechtsrahmen für eine regulierte Datenökonomie besteht damit bereits. Darüber hinaus sind im Zivilrecht Verträge mit Daten als Gegenleistung Teil des bürgerlichen Rechts geworden (§§ 327 ff. BGB), was die rechtliche Anerkennung des Werts von Daten weiter und die Möglichkeit des Austauschs von Daten und Gegenleistung unterstreicht.