Deutscher Bundestag **Drucksache 19/26538**

19. Wahlperiode 09.02.2021

Antrag

der Abgeordneten Manuel Höferlin, Stephan Thomae, Mario Brandenburg (Südpfalz), Grigorios Aggelidis, Renata Alt, Nicole Bauer, Dr. Jens Brandenburg (Rhein-Neckar), Sandra Bubendorfer-Licht, Dr. Marco Buschmann, Britta Katharina Dassler, Dr. Marcus Faber, Daniel Föst, Otto Fricke, Thomas Hacker, Reginald Hanke, Peter Heidt, Katrin Helling-Plahr, Markus Herbrand, Torsten Herbst, Dr. Gero Clemens Hocker, Dr. Christoph Hoffmann, Reinhard Houben, Ulla Ihnen, Olaf in der Beek, Gyde Jensen, Dr. Christian Jung, Pascal Kober, Konstantin Kuhle, Ulrich Lechte, Michael Georg Link, Dr. Martin Neumann, Dr. h. c. Thomas Sattelberger, Dr. Wieland Schinnenburg, Frank Sitta, Dr. Hermann Otto Solms, Dr. Marie-Agnes Strack-Zimmermann, Benjamin Strasser, Katja Suding, Manfred Todtenhausen, Gerald Ullrich, Katharina Willkomm und der Fraktion der FDP

Datenpolitik für Selbstbestimmung, Wettbewerb und Innovation

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

1. Daten stehen im Zentrum der Freiheitsfragen, die unsere Zukunft prägen werden. Sie sind zentrales Wirtschaftsgut, Quelle der Inspiration sowie Ursprung politischer Macht und gesellschaftlicher Teilhabe. Ein zukunftsfähiger Rahmen für eine umfassende Datenpolitik sollte deshalb einen Bogen über die Themenbereiche Datenschutz, Datenrecht und Datenwirtschaft spannen und zu diesem Zweck die folgenden Ziele in den Blick nehmen: die Selbstbestimmung des Einzelnen im digitalen Raum zu stärken (Datenautonomie), einen funktionierenden Wettbewerb um Daten und aufgrund von Daten zu ermöglichen (Datenökonomie) sowie die Nutzbarmachung von Daten für Innovationen auf vielfältigen Ebenen zu fördern (Daten als Innovationstreiber).
2. Bevor Rahmenbedingungen für eine zukunftsfähige Datenpolitik geschaffen werden können, bedarf es einiger Grundsatzentscheidungen. Die wichtigste Weichenstellung dabei ist die Unterscheidung von personenbezogenen Daten und Daten ohne Personenbezug. Die Entscheidung, ob ein Datensatz oder einzelne Datenpunkte, aus denen sich ein Datensatz zusammensetzt, Personenbezug haben, ist jedoch in der Praxis häufig nicht trivial. Um Rechtssicherheit zu bieten, braucht es eine klare Wertentscheidung dahingehend, dass Daten, die zwar unter Mitwirkung von Personen erzeugt wurden und damit zumindest für eine logische Sekunde Personenbezug aufweisen, aber im Folgenden nicht für die Verwendung mit Personenbezug gedacht sind, aus der Definition personenbezogener Daten herausgehalten werden. Somit wären Datensätze, in denen sich kein Datenpunkt

mit Personenbezug mehr befindet oder auch Datensätze, bei denen ein nur vorübergehender Personenbezug zum nächstmöglichen Zeitpunkt entfernt wird, als nicht personenbezogene Daten zu verstehen. Als Beispiel hierfür können etwa Sensordaten dienen, die in einem Fahrzeug Informationen über die Einschlagtiefe einer hydraulischen Vorrichtung aufzeichnen und deshalb Aufschluss darüber geben können, wo sich auf der genutzten Fahrbahn Schlaglöcher befinden. Hierbei muss eine Re-Identifikation durch automatisierte und ausreichend starke Anonymisierungsverfahren sowie klare Sanktionierungsmöglichkeiten effektiv unterbunden werden. Zudem sollte die mitwirkende Person immer ein Nutzungsrecht an den erzeugten Daten erlangen (Datenrecht). Für bestimmte, häufig auftretende Fallgruppen, sollte zudem konkretisiert werden, wann ein Personenbezug vorliegt. Reine Maschinendaten erhalten beispielsweise keinen Personenbezug dadurch, dass sie Rückschlüsse auf die Leistungsfähigkeit des Arbeitnehmers zulassen, der die Maschine bedient – außer, wenn sie gerade für diesen Zweck analysiert werden.

3. Für personenbezogene Daten sollte das Ziel der Datensparsamkeit und -minimierung auch in einer digital transformierten und immer mehr datengetriebenen Welt ein Leitmotiv sein, das aktiv zur Selbstbestimmung des Einzelnen beiträgt. Das Prinzip der Datenminimierung ist jedoch nicht als starre Zahl oder einengende Vorgabe zu verstehen, sondern passt sich flexibel den Erfordernissen des jeweiligen Zwecks der Datenverarbeitung an und befördert sogar die Weiterentwicklung der Möglichkeiten im Bereich der Datenanonymisierung und -pseudonymisierung, auch durch die Nutzung synthetischer Datensätze.
4. Eine weitere klare Entscheidung ist bei der Frage zu treffen, ob es Eigentum an Daten geben kann. Für personenbezogene Daten verbietet sich die Idee des Dateneigentums schon aufgrund der im Eigentumsbegriff angelegten Idee, dass die Hoheit über Daten unwiederbringlich an Dritte übertragen werden könnte, was der unveräußerlichen Menschenwürde widerspricht. Zudem bietet hier bereits das Datenschutzrecht einen Rechtsrahmen, der eindeutig die Verfügungsbefugnis, also das Recht andere von der Nutzung auszuschließen, selbst mit den Daten zu verfahren oder auch das Recht anderen Nutzungsbefugnisse einzuräumen, der betroffenen Person zuweist. Für Daten ohne Personenbezug fällt die Entscheidung jedoch ebenso klar aus, wenn man das eng miteinander verflochtene Dreiecksverhältnis bei der Verwertung von Daten (das sogenannte Nutzungsdreieck) betrachtet, bei dem sowohl Anbieter, Nutzerin und Nutzer als auch Dritte die Position des Datenproduzenten einnehmen können oder ein anderweitig starkes Interesse am Zugriff auf Daten existiert. Es kann demnach häufig keine interessengerechte und eindeutige Entscheidung geben, wer im Rahmen dieses Nutzungsdreiecks eine dauerhaft exklusive Rechtsposition im Umgang mit Daten erhalten soll.
5. Neben diesen Grundsatzentscheidungen gibt es im aktuellen Rechtsrahmen und der heute bereits gelebten Praxis im Umgang mit Daten wichtige Betätigungsfelder, die vorrangig bearbeitet werden müssen, um alle weiteren Überlegungen einer umfassenden Datenpolitik überhaupt zu ermöglichen. Hierzu gehört das im Rahmen der GWB-Novelle und auf europäischer Ebene bereits viel diskutierte Themenfeld des Zugangs zu Daten. Regelungen zum Datenzugang sichern zum einen Selbstbestimmung und Wettbewerb und sind zum anderen essenziell für die Ausarbeitung von Innovationen. Eine generelle Pflicht zur Datenteilung ist jedoch abzulehnen, denn Datenbestände sind kein Allgemeingut, sondern ein wirtschaftlicher Wert, deren Erhebung und Aufbereitung Investitionen voraussetzt. Dort wo punktuell der alleinige Zugang zu bestimmten Daten Innovationen hemmt und zum Wettbewerbshindernis wird, muss jedoch der kartellrechtliche Anspruch bestimmter Marktteilnehmer auf klar definierten, begrenzten Zugang zu diesen Daten, gegebenenfalls auch sektorspezifisch, konkretisiert werden, um für mehr Rechtssicherheit zu sorgen.

6. Darüber hinaus existiert mit der Datenportabilität, die sowohl für personenbezogene Daten gilt als auch in verschiedenen Bereichen bereits für Daten ohne Personenbezug, heute schon ein starkes Instrument, um Daten zugänglich zu machen und weiter zu verwerten. Um dem Instrument der Datenportabilität wirklich zum praktischen Durchbruch zu verhelfen, braucht es jedoch eine Einigung darauf, was der rechtlich bereits existierende Anspruch auf Herausgabe von Daten genau umfasst und innerhalb welcher Strukturen beziehungsweise anhand welchen Modells in einem einheitlichen Datenaustauschformat die Daten zur Verfügung gestellt werden müssen. Mittelfristig sollte die Selbstbestimmung der Nutzerinnen und Nutzer sowie der Wettbewerb durch eine Interoperabilität der Angebote gestärkt werden.
7. Ein weiterer Bereich, über den die Bedingungen für Datenzugang verbessert und gleichzeitig die Voraussetzung vieler Innovationen der Zukunft geschaffen werden können, ist die Ermöglichung und Einrichtung von Datenpools und Datendrehscheiben. Aktuell bestehen noch sowohl praktische als auch rechtliche Hindernisse (insbesondere im Kartellrecht), die eine Einrichtung eines gemeinsamen Datenpools und die Zusammenführung von Daten zu diesem Zweck erschweren. Dabei sind qualitativ hochwertige Daten im Bereich des Trainings künstlicher Intelligenz und der Erstellung besonders datenarmer Algorithmen entscheidend. Es reicht allerdings nicht, wie von der Bundesregierung vorgeschlagen, einen behördeninternen Datenpool zu errichten, an dem die Verwaltung gemeinsam arbeiten kann, oder den Begriff der Datenräume einzuführen. Die rechtlichen Bedingungen für die Einrichtung von Datenpools müssen insbesondere für die Anwendung durch Wirtschaft und Forschung geklärt werden. Die unterschiedlichen Motivationen, an einem Datenaustausch teilzunehmen, lassen sich über Datenpools alleine jedoch nicht abbilden. Nicht jeder Akteur kann in gleicher Weise zum Aufbau von Datenpools beitragen oder sein Interesse besteht möglicherweise nur darin, auf die Ergebnisse und Erkenntnisse aus der Auswertung großer Datenpools zuzugreifen. Deshalb ist ein wichtiger Baustein für einen verbesserten Datenzugang, wo dieser von allen Beteiligten gewünscht ist, um damit Innovationen auf Grundlage von Daten zu ermöglichen, der Aufbau von Strukturen über die nicht nur Daten zusammengeführt werden können, sondern auch die aus Daten gewonnenen Informationen gemeinsam ausgetauscht werden können. Zu solchen Datendrehscheiben könnten sich verschiedenste Akteure mit unterschiedlichen Beiträgen als Konsortium zusammenschließen und die so geschaffene Datenaustauschstruktur sogar für externe Nutzerinnen und Nutzer öffnen. Hierdurch soll der Austausch von Daten oder der reine Zugang zu Informationen zu fairen, zumutbaren und diskriminierungsfreien Bedingungen ermöglicht werden.
8. Der Staat sitzt selbst auf den größten Datenschätzen, die er entweder durch direkte Mitwirkung von Bürgerinnen und Bürgern erlangt hat oder die durch den Einsatz öffentlicher Ressourcen erstellt wurden. Deshalb muss die Öffentlichkeit auch grundsätzlich einen Anspruch auf Bereitstellung der betroffenen Daten als offene Verwaltungsdaten haben (Open Data). Der bisherige Rechtsrahmen zu Open Data sieht weder einen klaren Anspruch noch die maschinenlesbare Form der Bereitstellung vor und muss deshalb dahingehend weiterentwickelt werden, dass Daten in der Regel automatisch und in maschinenlesbarer Form zur Verfügung gestellt und nicht erst auf Antrag herausgegeben werden. Die Bereitstellung besonders hochwertiger Daten für die kommerzielle Nutzung in einem Lizenzsystem ist denkbar. Das Portal GovData des IT-Planungsrates, das auf Grundlage einer Verwaltungsvereinbarung mit dem Bund und zwölf Ländern betrieben wird, bietet bereits Zugang zu zahlreichen offen verfügbaren Verwaltungsdaten und soll deshalb als Plattform für alle weiteren Überlegungen zur Veröffentlichung von Open Data weiter ausgebaut werden. Die EU-Kommission unterstützt die

Strategie „Plan S“, welche sich dem langfristigen Ziel verpflichtet, wissenschaftliche Informationen und Erkenntnisse, die mit öffentlichen Mitteln gefördert wurden, öffentlich zugänglich zu machen. Die Bundesregierung ist dieser Strategie bisher nicht beigetreten und muss dies nachholen.

9. Im Bereich der Selbstbestimmung über personenbezogene Daten ergeben sich praktisch häufig Informationsasymmetrien oder Machtungleichgewichte zwischen Anbietern und Nutzerinnen sowie Nutzern von Daten. Gerade in diesen Konstellationen können Datentreuhänder einen Ausweg bieten, um eine missbräuchliche Verwendung von Daten auf der einen Seite und das Vertrauen der Nutzerinnen und Nutzer zur Bereitstellung ihrer Daten auf der anderen Seite sicherzustellen. Voraussetzung ist allerdings ein klarer Rechtsrahmen für Treuhänder, der die treuhänderischen Pflichten dahingehend konkretisiert, dass Datentreuhänder im besten Interesse der Nutzerinnen und Nutzer handeln müssen. Im selben Themenspektrum bewegt sich die Frage der Delegierbarkeit von Einwilligungen oder zumindest typisierten Entscheidungen über die Verwendung von personenbezogenen Daten. Beide Konzepte fallen in den Bereich der sogenannten „privacy enhancing technologies“. Die informationelle Selbstbestimmung als Schutzgut des Datenschutzes dient nicht nur als Abwehrrecht, sondern ist auch als Gestaltungsanspruch zu verstehen. Durch ein solches Verständnis wird sowohl eine effektive Verteidigung gegen den unbefugten Zugriff auf personenbezogene Daten sichergestellt als auch eine souveräne Entscheidung über die Nutzung der eigenen Daten gewährleistet. Deshalb stellen der Einsatz von Datentreuhändern und auch die Möglichkeit zur technischen Delegierung von Entscheidungen den Stand der Technik bei der Verarbeitung von personenbezogenen Daten dar.
10. Ziel muss es sein, die betroffenen Personen in die Lage zu versetzen, effektiv selbst über die Verarbeitung ihrer Daten zu entscheiden. Dazu gehört, dass die informationelle Selbstbestimmung der Nutzerinnen und Nutzer von Herstellern und Anbietern sowie weiteren Verantwortlichen bereits beim Design von Hard- und Software berücksichtigt wird (Datenschutz durch Technik – privacy by design) und datenschutzfreundliche Voreinstellungen Standard werden (privacy by default). Deutlich wird diese Notwendigkeit beim Nutzungsverhalten im Internet: Irgendwann klicken Nutzerinnen und Nutzer genervt jedes Cookie-Banner an; besser wäre es, wenn sie im Browser selbst über das Tracking im Netz entscheiden und im Zweifel geschützt sind (siehe Antrag FDP-Bundestagsfraktion „Smart Germany – Souveränität der Nutzerinnen und Nutzer über ihre IT-Systeme gewährleisten“ auf Bundestagsdrucksache 19/14050). Auch beim Inhalt von datenschutzrechtlichen Einwilligungen müssen die Nutzerinnen und Nutzer darauf vertrauen können, dass sie – wie auch sonst im Rechtsverkehr – mit fairen Bedingungen konfrontiert werden. Statt eines starren Koppelungsverbots brauchen wir daher eine AGB-Kontrolle, die Umfang, Zwecke und Dauer der Einwilligung in die Verarbeitung ihrer Daten einer Missbrauchskontrolle unterwirft und dahingehende Klauselverbote vorsieht.
11. Der Datenschutz wird häufig wahlweise als Innovationshemmnis oder Ursprung vielfältiger Probleme bei der Umsetzung von Ideen betrachtet. Dabei ist regelmäßig nicht der Datenschutz das Problem, sondern die uneinheitliche Anwendung des Rechtsrahmens für personenbezogene Daten aufgrund unseres föderalen Systems der Datenschutzaufsicht. Während es zwischen den Mitgliedstaaten auf europäischer Ebene seit der Einführung der DSGVO starke Kohärenzprinzipien gibt, die dazu führen, dass Zuständigkeiten eindeutig festgelegt und gemeinsame Rechtsansichten abgestimmt werden, haben wir in Deutschland bei der Datenschutzaufsicht immer noch ein kleinteiliges System, das zu häufig nicht zu einer föderierten Aufgabenteilung führt, sondern zu Verwirrung bei der Rechtsanwendung. Unser föderales System der Datenschutzaufsicht soll schon aufgrund des

Gesichtspunkts, dass die Datenschutzbehörden lokale Hilfestellungen bieten können und als niedrigschwellige Ansprechpartner dienen, nicht aufgegeben werden. Die Entscheidung einer Aufsichtsbehörde zu einem vorgelegten Sachverhalt sollte jedoch für das betroffene Unternehmen in der Praxis allgemeine Rechtssicherheit schaffen und einmal getroffene Entscheidungen zur Bewilligung von Verhaltensregeln nach Art. 40 DSGVO sollten für alle nationalen Datenschutzaufsichtsbehörden Bindungswirkung entfalten. Hierzu brauchen wir auf staatsvertraglicher Basis ein nationales Kohärenzverfahren.

12. Es ist zudem nicht hinnehmbar, wenn das Datenschutzrecht gegenüber Vereinen und KMUs durchgesetzt wird, nicht aber an den datenschutzrechtlichen Brennpunkten gegenüber den großen IT-Unternehmen. Dies liegt primär daran, dass hier für die Durchsetzung des Datenschutzrechts in den meisten Fällen die irische und luxemburgische Datenschutzbehörde zuständig sind, weil die europäischen Zentralen der großen IT-Unternehmen sich dort angesiedelt haben. Diese Behörden sind bereits nicht ausreichend ausgestattet, um der Aufgabe einer wirksamen Aufsicht nachkommen zu können, die sie im Interesse aller europäischen Bürgerinnen und Bürger ausüben muss. Die Bundesregierung muss sich daher gegenüber Irland und Luxemburg für eine ausreichende Ausstattung und konsequente Durchsetzung des europäischen Datenschutzrechts einsetzen und gegebenenfalls auch unionsrechtliche Schritte prüfen. Grundsätzlich haben die anderen europäischen Aufsichtsbehörden auch die Möglichkeit, im Rahmen des Europäischen Datenschutzausschusses das Tätigwerden einer nationalen Behörde zu erzwingen. Hiervon müssen sie aber auch Gebrach machen und dürfen keine falsche Rücksichtnahme an den Tag legen, sondern müssen bindende Entscheidungen treffen und ihre eigenen Befugnisse in eiligen Fällen auch nutzen.

13. Die Entscheidung des EuGH in der Rechtssache „Schrems II“ vom 16. Juli 2020 hat nach dem „Safe Harbor“-Mechanismus nun auch das „Privacy Shield“ als Grundlage des internationalen Datentransfers zwischen der EU und den USA gekippt sowie die Anwendung der Standarddatenschutzklauseln mit erheblichen Zweifeln belegt, die einer einfachen Anwendung entgegenstehen. Soweit sich diese Zweifel durch eine Weiterentwicklung der Standarddatenschutzklauseln beheben lassen, ist dieses Projekt mit Priorität von der EU-Kommission voranzutreiben. Politisch sind die Spielräume allerdings eng, weil die Entscheidung des EuGH auf der europäischen Grundrechte-Charta beruht und einziger Hebel eine Änderung des US-amerikanischen Nachrichtendienstrechts ist. Aufgrund der Bedeutung des transatlantischen Datenverkehrs sollten die EU-Kommission und die Mitgliedstaaten aber weiterhin versuchen, eine Einschränkung der exzessiven Überwachungsbefugnisse der US-Nachrichtendienste gegenüber Ausländern und eine Verbesserung der rechtlichen Stellung und des Rechtsschutzes für EU-Bürger zu erreichen. Da sich die gleichen Probleme auch im Datenverkehr mit anderen Ländern stellen (insbesondere China und Russland) ist es zur Aufrechterhaltung des internationalen Datenverkehrs von essenzieller Bedeutung, zumindest technische Möglichkeiten zum Austausch von Daten zu bieten. Hierzu gehört etwa eine zwingende Vorgabe zur Verschlüsselung von Daten während der Übertragung (siehe hierzu Antrag FDP-Bundestagsfraktion „Recht auf Verschlüsselung – Privatsphäre und Sicherheit im digitalen Raum stärken“ auf Bundestagsdrucksache 19/5764). Die im „Data Governance Act“ der EU-Kommission angedachten Datenräume sollten überdies in den weiteren Beratungen des Verordnungsentwurfs um eine internationale Dimension erweitert werden. Auch wenn der Bedarf an Datenlokalisierung und damit europäischen Speicherstrukturen für Daten gerade aufgrund der anhaltenden Rechtsunsicherheit steigen wird, ist es aus Sicht eines Europäischen Wirtschaftsraums unerlässlich internationale Datentransfers weiter zu ermöglichen. Mittelfristig sollte Deutschland das Projekt

der Festigung des Rechts auf informationelle Selbstbestimmung als Menschenrecht und die Entwicklung von Mindeststandards für staatliche Überwachungsmaßnahmen auch auf internationaler Ebene vorantreiben, etwa durch eine Initiative für ein Zusatzprotokoll zu Art. 17 des Internationalen Paktes für bürgerliche und politische Rechte.

14. Die Fraktion der FPD im Bundestag fordert schon seit ihrem „Programm zur Beschleunigung der Digitalisierung in Deutschland“ (siehe Bundestagsdrucksache 19/2991) vom 27.06.2018, das bestehende Recht zu einem modernen Datenrecht fortzuentwickeln, welches gleichzeitig innovative digitale Zukunftstechnologien und Geschäftsmodelle ermöglicht und die Persönlichkeitsrechte der Bürgerinnen und Bürger schützt. Dementsprechend wurde schon damals eine Ergänzung des Rechtsrahmens dahingehend gefordert, dass die Bandbreite von Datenschutz und Datennutzung in einer digitalisierten Welt abgebildet wird. Die EU-Kommission hat im Februar 2020 eine europäische Datenstrategie vorgelegt und arbeitet mit dem „Data Governance Act“ und dem „Digital Markets Act“ am Rechtsrahmen für die datengetriebene Wirtschaft und Gesellschaft von morgen. Die Bundesregierung hat am 27.01.2021 nun ihrerseits eine Datenstrategie vorgelegt, mit der sie allerdings vor allem den aktuellen Diskussionsstand zur Datenpolitik widergibt. Dies ist symptomatisch für die geringe Geschwindigkeit, die sie in der Digitalpolitik an den Tag legt.

II. Der Deutsche Bundestag fordert die Bundesregierung vor diesem Hintergrund dazu auf,

die Umsetzung wichtiger Weichenstellungen im Bereich der Datenpolitik nicht in die nächste Legislaturperiode zu verschieben und deshalb die folgenden konkreten Maßnahmen zeitnah und jedenfalls noch in der laufenden Legislaturperiode zu ergreifen:

1. Im Bereich der Datenautonomie:

- Den Einsatz von Datentreuhändern zur Förderung der Selbstbestimmung über personenbezogene Daten bei auftretenden Informationsasymmetrien oder Machtungleichgewichten in sogenannten „Vertrauensmärkten“ zwischen Anbietern und Nutzerinnen sowie Nutzern von Daten voranzubringen. Zu diesem Zweck soll sich die Bundesregierung bei der Aushandlung des „Data Governance Act“ auf europäischer Ebene dafür einsetzen, bei der Konkretisierung der Vorgaben für „Dienste für die gemeinsame Datennutzung“ konkrete treuhänderische Pflichten einzuführen, um sicherzustellen, dass die Datentreuhänder im besten Interesse der Nutzerinnen und Nutzer handeln müssen. Für Datentreuhänder, die von staatlichen Stellen eingesetzt werden, sollen im Rahmen der auch in der Datenstrategie der Bundesregierung vorgesehenen Vorreiterrolle des Staates die Governance-Strukturen der Treuhänder offengelegt werden, um so Anschauungsmaterial für die Nachahmung in anderen Fällen zu liefern;
- sich bereits vor der nächsten Evaluierung der DSGVO auf europäischer Ebene für die Ergänzung von Regelungen zur Ermöglichung der Delegierbarkeit von datenschutzrechtlichen Einwilligungen oder zumindest typisierten Entscheidungen einzusetzen. So soll die Rechtswahrnehmung anhand klarer Vorgaben wirksam von Dritten oder technischen Vorrichtungen übernommen werden können. Über die rechtliche Klarstellung zur Frage der Delegierbarkeit von Entscheidungen hinaus fordert der Deutsche Bundestag die Bundesregierung dazu auf, in ihrem eigenen Zuständigkeitsbereich für einzelne Fragestellungen, wie etwa den Einsatz von Cookie-Einwilligungs-Assistenten, ihrer Vorreiterrolle gerecht zu werden und datenschutzfreundliche Voreinstellungen flächendeckend zur Anwendung zu bringen;

- durch die Vergabe von Pilotprojekten für öffentliche Stellen und die Finanzierung von Forschungsvorhaben im Rahmen der zur Verfügung stehenden Haushaltsmittel die Weiterentwicklung von sogenannten „privacy enhancing technologies“ sowie Techniken zur anonymisierten Aufbereitung oder Modellierung synthetischer Datensätze voranzubringen;
- einen Gesetzentwurf zur Ergänzung der Vorschriften zur AGB-Kontrolle im BGB vorzulegen, welcher sich insbesondere auf die Überprüfbarkeit datenschutzrechtlicher Einwilligungen in Nutzungsbedingungen bezieht. Die Überprüfbarkeit muss sich zum einen auf eine Missbrauchskontrolle in Bezug auf den Umfang, die Zwecke und die Dauer eingeholter Einwilligungen in die Verarbeitung von Daten der Nutzerinnen und Nutzer beziehen und zum anderen explizite Klauselverbote in Bezug auf die Einwilligung in die Verarbeitung personenbezogener Daten vorsehen;

2. im Bereich der Datenökonomie:

- in der Debatte um Datenzugangsrechte eine klare Haltung gegen allgemeine Datenteilungspflichten einzunehmen und eventuelle Überlegungen zu sektorspezifischen Zugangsregeln auch nicht als „Datenteilungspflichten“ zu bezeichnen. Darüber hinaus fordert der Deutsche Bundestag die Bundesregierung dazu auf, sich im Rahmen der Erarbeitung des „Digital Markets Act“ und des „Data Governance Act“ auf europäischer Ebene für die Verankerung der Ermöglichung des Datenzugangs über sogenannte Datendrehscheiben einzusetzen, auch unabhängig von den bereits angedachten Regelungen von Verpflichtungen für sogenannte „Gatekeeper“. Dies könnte eine konkrete Umsetzung des Ziels sein, Zugang zu Informationen zu fairen, zumutbaren und diskriminierungsfreien Bedingungen zu gewähren;
- im Rahmen der deutschen Beteiligung am GAIA-X-Projekt die Einführung von Strukturen für Datendrehscheiben und gemeinsame Datenpools voranzutreiben und sich dafür einzusetzen, dass die aufgebauten Strukturen in den Bereichen Wirtschaft, Staat (über die beteiligten Behörden), Gesundheit und Bildung miteinander verknüpft werden können. So soll sichergestellt werden, dass in Zukunft nicht Parallelentwicklungen in verschiedenen Bereichen stattfinden, wenn in einem anderen Bereich bereits Lösungen für dieselbe Problemstellung vorhanden sind. Der Staat soll seiner Vorreiterrolle dadurch gerecht werden, dass er das Portal GovData als Datenpool an GAIA-X anschließt;
- um internationale Datentransfers auch nach Schrems II rechtssicher zu ermöglichen, sich neben der Aushandlung eines neuen rechtlichen Schutzmechanismus zur vereinfachten Datenübermittlung in Drittstaaten wie die USA für technische Lösungen des Problems der unterschiedlichen Datenschutzniveaus dies- und jenseits des Atlantiks sowie in anderen Rechtsräumen der Welt einzusetzen. Hierzu fordert der Deutsche Bundestag die Bundesregierung dazu auf, einen Gesetzentwurf vorzulegen, mit dem Telekommunikations- und Telemediendiensteanbieter dazu verpflichtet werden, ihre Dienste als Standard abhörsicher (Ende-zu-Ende verschlüsselt) anzubieten;

- einen Gesetzentwurf vorzulegen, mit dem die Möglichkeit eines nationalen Kohärenzverfahrens nach Vorbild des in der DSGVO für die europäische Ebene vorgesehenen Systems in das BDSG eingeführt wird, um zu einer einheitlichen Anwendung datenschutzrechtlicher Vorschriften im föderalen System der deutschen Datenschutzaufsicht zu gelangen, ohne dabei das Datenschutzniveau abzusenken. Das Kohärenzverfahren muss im Folgenden auf staatsvertraglicher Ebene von den Aufsichtsbehörden verankert werden. Teil des Kohärenzverfahrens soll zum einen die Bindungswirkung in Bezug auf Entscheidungen zu einzelnen vorgelegten Sachverhalten sein und zum anderen eine verpflichtende Anerkennung bereits bewilligter Verhaltensregeln nach Art. 40 DSGVO durch die einzelnen Aufsichtsbehörden;

3. im Bereich von Daten als Innovationstreiber:

- sich bereits vor der nächsten Evaluierung der DSGVO auf europäischer Ebene für die Anpassung der Definition personenbezogener Daten in Art. 4 Nr. 1 DSGVO einzusetzen, um eine trennscharfe Unterscheidung von personenbezogenen Daten und Daten ohne Personenbezug zu ermöglichen und damit Rechtssicherheit darüber zu schaffen, welche Sachverhalte nicht unter die DSGVO fallen. Neben einer allgemeinen Definition, wann Datensätze keinen Personenbezug mehr aufweisen, ist zum Zweck einer einheitlichen Rechtsanwendung die Einführung einer Positivliste plastischer Regelbeispiele anzustreben. In Zusammenhang mit der definitorischen Abgrenzung von Datensätzen mit und ohne Personenbezug ist jedoch sicherzustellen, dass die an der Entstehung von Daten mitwirkenden Personen immer ein Nutzungsrecht an den erzeugten Daten erlangen (Datenrecht);
- der Datenportabilität als Instrument zur Gewährung von Datenzugang zum Durchbruch in der Praxis zu verhelfen. Im Rahmen der Vorreiterrolle des Staates sollten deshalb überall dort, wo staatliche Stellen dies selbst beeinflussen können, Konzepte zur Umsetzung der Datenportabilität zur Anwendung kommen, die zu einer Nutzung dieses Instruments anregen. Darüber hinaus fordert der Deutsche Bundestag die Bundesregierung dazu auf, darauf hinzuwirken, dass über die bekannten Normungsgremien Standards für den Datenaustausch erarbeitet werden;
- bestehende rechtliche – insbesondere kartellrechtliche – Hürden für Datenkooperationen, den Aufbau gemeinsamer Datenpools oder das Betreiben gemeinsamer Datendrehscheiben abzubauen. Staatliche Stellen sollten auch hier ihrer Vorreiterrolle gerecht werden, indem sie selbst Datendrehscheiben betreiben, über welche sie insbesondere für Externe den Zugang zu staatlichen Datenpools in einer Form ermöglichen, die es ihnen ermöglicht, eine Auswertung der dort vorhandenen Datensätze selbst vorzunehmen oder an den staatlichen Auswertungsergebnissen teilhaben zu können;
- die Bemühungen im Bereich Open Data schnell und umfassend voranzubringen. Damit Bund, Länder, Kommunen und alle weiteren öffentlichen Stellen an einem Strang ziehen, muss ein „Open Data Pakt“ zwischen allen staatlichen Ebenen vereinbart werden. Im Rahmen dessen fordert der Deutsche Bundestag die Bundesregierung dazu auf, einen Gesetzentwurf vorzulegen, mit dem ein Bundestransparenzgesetz (angelehnt an das Transparenzgesetz Hamburg) eingeführt und das Grundprinzip der Veröffentlichung von Open Data im eGovernment-Gesetz gestärkt wird. Um ihrer Vorreiterrolle gerecht zu werden, soll sich auch die Bundesregierung den Zielen des „Plan S“ verpflichten und das Portal GovData schon heute stärken, indem sie beginnt, offene Verwaltungsdaten auch ohne bereits rechtlich normierten Anspruch dort umfassend zu veröffentlichen. Zudem sollte sie sich das Ziel setzen, den Quellcode von Software, die von staatlichen Einrichtungen oder unter Einsatz von öffentlichen Ressourcen entwickelt wird, möglichst zu veröffentlichen;

- die Vermittlung grundlegender Fähigkeiten im Umgang mit Daten in den bildungspolitischen Fokus zu rücken. Sowohl im Bereich der schulischen Bildung, der Weiterbildung und des lebenslangen Lernens als auch bei der Ausgestaltung von Ausbildungsinhalten und Lehrplänen muss das Thema „data literacy“ künftig stärker berücksichtigt werden. Ein erster Schritt in die richtige Richtung wäre die Adaptierung des finnischen „Elements of ai-Kurses“ auf verschiedenen Ebenen auch für Deutschland, wie von der FDP-Fraktion bereits im Antrag „Smart Germany: Deutschland digital stärken – Onlinekurs „Künstliche Intelligenz“ initiieren“ (auf Bundestagsdrucksache 19/14034) gefordert.

Berlin, den 9. Februar 2021

Christian Lindner und Fraktion

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333