Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Vortrag

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Ministerialdirektor Jürgen H. Müller,
Leitender Beamter

„Digitalisierung braucht Datenschutz“

bei den Berliner Anwendertagen 2020

Berlin, den 13. Februar 2020

Es gilt das gesprochene Wort

Meine sehr geehrten Damen und Herren,

I. Einleitung

Ich freue mich, bei den Berliner Anwendertagen zu Gast zu sein und zum Abschluss die Perspektive des Datenschutzes in die Diskussion einzubringen. Ich hoffe, dass die bisherigen Foren Grundlage für eine angeregte Diskussion in der Mittagspause waren und ich Sie nicht aus dem berühmten Suppenkoma holen muss.

Die Digitalisierung schreitet in allen Lebensbereichen voran und macht auch vor der Bundesverwaltung nicht Halt. Hier laufen verschiedenste Digitalisierungsprojekte. Sie beginnen bei Online-Formularen für BAföG-Anträge und reichen bis hin zum Einsatz von Algorithmen bei der Gefahrenprävention. Diese Entwicklung, die wir hier erleben, wird in den kommenden Jahren fortschreiten.

In der öffentlichen Diskussion geht es beim Thema Digitalisierung oft um die Themen künstliche Intelligenz und maschinelles Lernen. Dies sind Themen, die auch Teile der öffentlichen Verwaltung beschäftigen, wie beispielsweise die aktuelle Diskussion um die automatisierte Gesichtserkennung im öffentlichen Raum zeigt.

In der Praxis sind viele Behörden derzeit jedoch mit profaneren Digitalisierungsprozessen beschäftigt, etwa der Einführung einer elektronischen Aktenverwaltung oder der Verlagerung der Serverstrukturen in „Cloud-Lösungen“. Ein Großprojekt, das Bund, Länder und Kommunen betrifft, ist die **Einrichtung eines gemeinsamen Bürgerportals**. Hier sollen die Bürgerinnen und Bürger über eine zentrale Plattform verschiedenste Verwaltungsleistungen in Anspruch nehmen können.

Und dies unabhängig davon, ob die Leistungen in der Zuständigkeit der Kommunen, des Landes oder des Bundes liegen.

II. Automatisierte Entscheidungen in der Verwaltung

Auch wenn der Einsatz algorithmischer Systeme und künstlicher Intelligenz in der Verwaltung bisher noch eher eine untergeordnete Rolle spielt, ist davon auszugehen, dass sich dies in den nächsten Jahren ändern wird.

Die Verwaltung birgt ein großes Potential für den Einsatz algorithmischer Systeme. So ist es denkbar, dass Routinefälle künftig nicht mehr durch Verwaltungsmitarbeiter, sondern durch speziell entwickelte Programme bearbeitet werden könnten. Auch auf gesetzgeberischer Seite wurde dieses Potenzial bereits erkannt. Nach § 35a des Verwaltungsverfahrensgesetzes dürfen **Verwaltungsakte** automatisiert erlassen werden, wenn eine Rechtsvorschrift dies zulässt und weder ein Ermessens- noch ein Beurteilungsspielraum bestehen.

In der **Steuerverwaltung** kommen bereits automatisierte Entscheidungsverfahren zum Einsatz. Nach § 155 Absatz 4 der Abgabenordnung können Steuererklärungen voll automatisiert bearbeitet und Bescheide automatisiert versendet werden. Von dieser Möglichkeit macht die Steuerverwaltung in Routinefällen seit 2018 Gebrauch.

Für den weiteren Einsatz algorithmischer Systeme bieten sich insbesondere alle Bereiche der Leistungsverwaltung an. Die erforderlichen Daten und Unterlagen werden eingereicht, automatisiert geprüft und anschließend wird die entsprechende Leistung gewährt.

Doch ist im Bereich der Eingriffsverwaltung größere Vorsicht geboten, denn diese ist immer mit dem **Eingriff in Grundrechte** verbunden. In sensiblen Feldern sollten deshalb ausschließlich klassische, deterministische Algorithmen zum Einsatz kommen, denn nur so kann die Entscheidungsfindung durch den Algorithmus klar nachvollzogen werden.

Verfahren des maschinellen Lernens sollten insbesondere in der Eingriffsverwaltung nicht zum Einsatz kommen. Diese werden dadurch charakterisiert, dass sie analytische Modelle automatisiert erstellen. Durch die Verwendung von Algorithmen, die wiederholend aus Daten lernen, sind diese Programme in der Lage, versteckte Erkenntnisse zu gewinnen, ohne explizit programmiert worden zu sein. So ist es nachträglich nicht immer möglich, die Entscheidungsfindung des Algorithmus nachzuvollziehen. Dies jedoch ist für die Legitimation und für eine nachgelagerte Überprüfung von Grundrechtseingriffen unabdingbar.

III. Datenschutz mitdenken

Egal, welche digitalen Anwendungen zum Einsatz kommen: Durch die digitalen Technologien dürfen unsere grundlegenden Werte, Rechte und Freiheiten nicht verändert werden. Vielmehr müssen diese bei der Entwicklung und dem Einsatz digitaler Technologien mitgedacht werden. Dies bedeutet, dass auch der **Datenschutz von Anfang an mitzudenken** ist.

Als langjähriger Mitarbeiter und Leitender Beamter des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit habe ich schon zahlreiche Digitalisierungsprojekte begleitet. Eine wichtige Lehre, die ich aus diesen Erfahrungen gezogen habe, ist, den **Datenschutz** wirklich von **Beginn an** zu berücksichtigen. Viele datenschutzrechtliche Probleme, die im Verlauf eines Projektes auftauchen, hätten vermieden werden können, wenn datenschutzrechtlicher Sachverstand von Anfang an mit ins Boot geholt worden wäre.

Sobald ein Digitalisierungsprojekt in einer Behörde in Angriff genommen wird, empfiehlt es sich dringend, den Datenschutzbeauftragten der Behörde in Kenntnis zu setzen und laufend zu beteiligen. So können datenschutzrechtliche Fragestellungen frühzeitig erkannt und gelöst werden, statt sie in einem späteren Prozess aufwendig nachzubessern. Ein Beispiel ist die Implementierung von Löschregeln. Aus unserer Beratungs- und Kontrollpraxis wissen wir, dass in der Verwaltung immer wieder Anwendungen zum Einsatz kommen, die über keine Löschroutine verfügen.

Einer der zentralen Grundsätze des Datenschutzrechts ist die **Datensparsamkeit**. Personenbezogene Daten dürfen nur so lange gespeichert werden, wie dies für die Aufgabenerfüllung erforderlich ist. Bei allen Anwendungen, die auch personenbezogene Daten beinhalten, sind daher die Möglichkeit zur Löschung und entsprechende zeitliche Vorgaben unabdingbare Voraussetzung für eine datenschutzkonforme Anwendung.

Löschfunktionen nachträglich zu programmieren stellt die Programmierer regelmäßig vor große Herausforderungen. Zum Wohl des Datenschutzes, aber auch aus Effizienz- und Kostengründen, müssen die aus dem Datenschutzrecht folgenden Anforderungen bei neuen digitalen Anwendungen von Anfang an implementiert werden.

Bei inhaltlichen Fragen stehen den betroffenen Behörden meine Mitarbeiterinnen und Mitarbeiter oder meine Kolleginnen und Kollegen aus den Landesdatenschutzbehörden als kompetente Partner beratend zur Seite.

IV. DSGVO als rechtlicher Maßstab

Wie eben dargelegt, sollten Datenschutzaspekte bei Digitalisierungsprojekten von Anfang an mitgedacht werden. Dies ist übrigens nicht nur mein hehrer Wunsch als Vertreter des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, sondern eine rechtliche Vorgabe. Die Datenschutz-Grundverordnung hat hierfür die Begriffe „**Privacy by Design and Default**“ aufgegriffen. Oder auch: Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen.

Dies sind keine neuen Begriffe. Im Rahmen der DSGVO erlangen sie jedoch neue Bedeutung und sind in Art. 25 der DSGVO verankert.

Mit der DSGVO haben wir eine rechtlich unmittelbar verbindliche und verlässliche Grundlage für die Mitgliedstaaten der Europäischen Union. An sie ist die Verwaltung auch im Rahmen ihrer Digitalisierungsbemühungen gebunden. Die DSGVO stellt hinreichend klar, was wir von IT-Systemen erwarten können und müssen.

Wie in meinem Beispiel der Datenlöschung ist auch bei der ursprünglichen Speicherung personenbezogener Daten in digitalen Anwendungen der **Grundsatz der Datenminimierung** zwingend zu berücksichtigen. Niemand hat das Recht, personenbezogene Daten zu erheben, die er für die Aufgabenerfüllung nicht benötigt.

Es ist daher immer darauf zu achten, nur die Daten zu erheben, die wirklich benötigt werden. Eine Anforderung, die im Design von IT-Anwendungen und Fachverfahren leider nicht immer berücksichtigt wird.

Die situationsgerechte **Anonymisierung oder Pseudonymisierung** personenbezogener Daten ist hierfür ein sinnvolles Instrument. Dies gilt insbesondere für eine datenschutzkonforme Datennutzung im Bereich von KI-Anwendungen. Auch Modelle des dezentralen Lernens oder datenschutzkonforme „data spaces“ ermöglichen zahlreiche Formen der Datennutzung ohne Personenbezug.

Ein weiterer zentraler Begriff in diesem Zusammenhang ist die **Datenschutz-Folgenabschätzung**. Artikel 35 DSGVO verlangt sie in den Fällen, in denen ein Verarbeitungsvorgang mit einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen einhergeht.

Soll eine neue Anwendung zum Einsatz kommen, muss stets im Vorfeld Artikel 35 DSGVO berücksichtigt werden. Die Datenschutz-Folgenabschätzung ist zwingend vor dem Einsatz der Anwendung durchzuführen. Sie ist beispielsweise bei der Verarbeitung sensitiver Daten nach Artikel 9 DSGVO – wie Gesundheitsdaten –, beim Einsatz neuer Technologien oder bei Datentransfers in außereuropäische Staaten notwendig. Die Aufsichtsbehörden in Bund und Ländern halten hier Listen von Verarbeitungsvorgängen bereit, bei denen in jedem Fall eine Datenschutz-Folgenabschätzung durchzuführen ist.

Transparenz ist beim Einsatz algorithmischer Systeme wesentlich. Die Gesetzesbindung der hoheitlichen Gewalt verlangt, dass staatliche Entscheidungen transparent und begründbar sind. Es ist daher unverzichtbar, dass die staatlichen Stellen über aussagekräftige und umfassende Informationen zu der von ihnen durchgeführten Datenverarbeitung und den eingesetzten Systemen verfügen. Diese sollten, soweit rechtlich möglich, veröffentlicht werden. Das hat auch die Konferenz der Informationsfreiheitsbeauftragten in Deutschland gefordert.[1]

[1] Positionspapier „Transparenz der Verwaltung beim Einsatz von Algorithmen für gelebten Grundrechtsschutz unabdingbar“, 36. IFK 2018

Dies sind nur einige Aspekte, die für einen datenschutzkonformen Einsatz digitaler Anwendungen zu berücksichtigen sind.

V. Datenschutz als Bremsschuh oder doch nicht Wettbewerbsvorteil?

Meine sehr geehrten Damen und Herren, es gibt zwei Fragen, die ich bzw. meine Behörde immer wieder höre:

1. Ist es angesichts der neuen Möglichkeiten, die die Digitalisierung bietet, wirklich sinnvoll, an den datenschutzrechtlichen Vorgaben festzuhalten?

   und

2. Bremst der Datenschutz nicht den technologischen Fortschritt, die wirtschaftliche Entwicklung und schreckt so Investoren ab?

Die Sichtweise, die hinter diesen Fragen steht, halte ich für gefährlich und falsch.

Uns Datenschutzbeauftragten kommt bei der Digitalisierung eine besondere Aufgabe zu: Wir müssen die technische Entwicklung konstruktiv begleiten und als **Garant für die Wahrung der Grundrechte** einstehen. Wir müssen unsere fachliche Kompetenz zuverlässig dafür einsetzen, neue und grundrechtskonforme Lösungen zu finden.

Hohe IT-Sicherheitsstandards und Datenschutzkonformität sind zentrale Qualitätsmerkmale. Sie schaffen **positive Alleinstellungsmerkmale** am Markt. Deutschland und Europa haben hier eine hervorragende Ausgangssituation. Wir können weltweit Marktführer bei sicheren und datenschutzkonformen Produkten und Dienstleistungen werden.

Ein starker Datenschutz ist unabdingbar für eine ethische und gerechte Ausgestaltung unserer digitalen Zukunft. Dies betonte auch die **Datenethikkommission** – ein von der Bundesregierung in Sachen Digitalpolitik eingesetzes Expertengremium – in ihrem Ende 2019 vorgelegten Abschlussgutachten. Es ist ein Irrglaube, dass es der Digitalisierung helfe, möglichst wenig zu regulieren und bestehende gesetzliche Vorgaben weitestgehend abzuschaffen. Wir haben einen innovativen Rechtsrahmen mit wichtigen und richtigen Leitplanken. Die Datenschutzgrundverordnung wird derzeit weltweit als Referenz und Blaupause für neue Rechtsvorgaben herangezogen.

Regulierung dient dazu, die Werte unserer Rechtsordnung zu gewährleisten und Grundrechte zu schützen. Daher muss Regulierung dort ansetzen, wo die Gefahren für die Rechtsgüter besonders hoch sind. Nachschärfung im Datenschutzrecht muss dort ansetzen, wo Gefahren für die Rechtsgüter des Einzelnen oder der Allgemeinheit drohen. Dies betrifft beispielsweise klarere Vorgaben und mehr Transparenz bei Profilbildungen, das Verbot von Algorithmen mit unvertretbarem Schädigungspotenzial oder spezifische Regelungen zum Datenhandel.

VI. Weiterentwicklung des Datenschutzrechts

Die Datenschutz-Grundverordnung als Basis europäischen Datenschutzrechts dient dem Schutz der informationellen Selbstbestimmung der Bürgerinnen und Bürger. Dieses Grundrecht gilt auch im digitalen Zeitalter und gewinnt gerade aufgrund neuer Speicher- und Auswertungsmöglichkeiten an Bedeutung.

Die DSGVO bietet eine gute Basis für den Schutz der informationellen Selbstbestimmung in Zeiten der Digitalisierung. Aber es gibt durchaus auch **Korrektur- und Nachbesserungsbedarf**. Aufgrund der oft offenen Formulierungen im Gesetzestext der DSGVO bestehen an manchen Stellen noch Unklarheiten. Hier müssen die Aufsichts- und die Rechtspraxis in der Zukunft für Konkretisierung sorgen, damit alle Beteiligten wissen, an welche Standards sie sich in puncto Datenschutz halten müssen und worauf sie sich verlassen können.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit setzt sich sowohl in Deutschland als auch auf europäischer Ebene dafür ein, dass die Aufsichtsbehörden diese Unklarheiten durch abgestimmte Auslegungshilfen beseitigen. Es werden und wurden auf europäischer Ebene bereits zahlreiche Leitlinien zur Auslegung der DSGVO erarbeitet und auch die deutsche Datenschutzkonferenz hat verschiedene Kurzpapiere und Orientierungshilfen zur DSGVO veröffentlicht. Diese stehen bei Bedarf auf der Internetseite des BfDI zum Abruf bereit.

Hinsichtlich der **Fortentwicklung der DSGVO** möchte ich mich auf drei Aspekte konzentrieren: Dies sind:

1. die Regulierung von Algorithmen,

2. verbesserte Vorschriften zu Profilbildung und Scoring sowie

3. mehr Pflichten für die Anbieter von digitalen Produkten und Anwendungen.

a. Regulierung Algorithmen

Im Bereich der Algorithmen und der künstlichen Intelligenz bedarf es auch aus Datenschutzsicht einer Ergänzung des Rechtsrahmens auf europäischer Ebene. Datenschutz soll technische Innovationen möglich machen, gleichzeitig aber auch Fehlentwicklungen vorbeugen. Regulierung sollte – wie bereits gesagt – dort ansetzen, wo Gefahren für die Rechtsgüter des Einzelnen oder der Allgemeinheit drohen.

Wie auch dem Gutachten der Datenethikkommission zu entnehmen ist, sollte für die Regulierung von Algorithmen ein **risikobasierter Ansatz** gewählt werden. Das bedeutet, dass bei den Algorithmen, durch deren Einsatz keine oder nur sehr geringe Gefahren für Rechtsgüter drohen, keine zusätzliche Regulierung erforderlich ist.

Wenn jedoch ein unvertretbares Schädigungspotenzial festgestellt wird, müssen im Einzelfall auch Verbote von Algorithmen ausgesprochen werden.

Im breiten Zwischenfeld kommen je nach Schädigungspotenzial verschiedene Ansätze, wie Codes of Conduct, Ex-post-Kontrollen oder aber auch Live-Schnittstellen mit Zugriffsmöglichkeiten für die zuständigen Aufsichtsbehörden in Betracht.

Bei der Bewertung eines algorithmischen Systems sind alle Komponenten zu berücksichtigen: Die eingesetzte Technik, das Anwendungsgebiet und die beteiligten menschlichen Akteure.

Auf europäischer Ebene werden derzeit ebenfalls regulatorische Maßnahmen in Bezug auf KI geprüft. Die Europäische Kommission soll Medienberichten zufolge insbesondere ein vorübergehendes Verbot von automatisierter Gesichtserkennung im öffentlichen Raum erwägen. Im Gespräch sind zudem spezielle Regeln für den Einsatz von KI durch die öffentliche Verwaltung und gesetzliche Vorgaben für Anwendungen mit hohem Risiko – beispielsweise im Gesundheitsbereich.[2]

[2] White Paper der EU-Kommission, veröffentlicht unter: https://g8fip1kplyr33r3krz5b97d1-wpengine.netdna-ssl.com/wp-content/uploads/2020/01/AI-white-paper-CLEAN.pdf

b. Regulierung Profiling

Bei der Profilbildung und insbesondere dem Scoring fordert der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit bereits seit Jahren mehr Transparenz. Auch unter der Datenschutz-Grundverordnung besteht die Problematik, dass der eigentliche Prozess der Profilbildung von den Normen der DSGVO – insbesondere Artikel 22 zur automatisierten Entscheidungsfindung – nur unzureichend erfasst wird. Hier ist aus meiner Sicht eine deutliche Nachschärfung der gesetzlichen Regeln erforderlich.

Die Datenethikkommission z.B. fordert „spezifische Kennzeichnungs-, Informations- und Auskunftspflichten bezüglich der Profilbildungen als solcher“. Diese Informationspflichten sollen nicht nur bei automatisierten Entscheidungen greifen, sondern generell beim Einsatz von Algorithmen zur Profilbildung.

In diesem Zusammenhang fordert die Datenethikkommission auch ein Recht auf einen „**digitalen Neuanfang**“ durch die Löschung der gebildeten Profile, beispielsweise mit Erreichen der Volljährigkeit.

Einen rechtstechnisch relativ einfach umzusetzenden Weg, den Schutz der Bürgerinnen und Bürger zu verbessern, schlagen die Aufsichtsbehörden des Bundes und der Länder in ihrem Erfahrungsbericht zur DSGVO vor: Die bereits vorhandenen Regelungen zur automatisierten Entscheidungsfindung in der DSGVO sollten auf die Bildung von Profilen erstreckt werden.

Momentan ist es nämlich so – um ein Beispiel aus dem Bereich des Scoring zu nennen –, dass beispielsweise die Schufa argumentiert, sie selbst träfe keine automatisierte Entscheidung, sondern stelle den Endkunden lediglich ein Profil – den Score – zur Verfügung.

Die Banken wiederum unterfallen häufig ebenfalls nicht den Schutzregelungen. Sie haben zumindest formal – etwa vor der Entscheidung über die Vergabe eines Kredites – einen Mitarbeiter als Entscheidungsinstanz.

Diese Lücke ließe sich schließen, indem bereits die Profilbildung als solche dem Verbot mit Erlaubnisvorbehalt des Art. 22 DSGVO unterstellt wird. Gleiches gilt für das Auskunftsrecht nach Art. 13 Abs. 2 DSGVO über „aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen“, um die Transparenz zu erhöhen.

c. Anbieter in die Pflicht nehmen

Als drittes nun zu den Pflichten der Anbieter digitaler Produkte und Anwendungen: Auch wenn neue Bereiche der Verwaltung digitalisiert werden sollen, stellt sich regelmäßig die Frage, ob bereits geeignete Anwendungen auf dem Markt sind oder ob eigene Anwendungen programmiert werden müssen.

Bei der Auswahl einer geeigneten Anwendung wäre sicher auch Ihren Behörden geholfen, wenn Datenschutz und Datensicherheit bereits vollumfänglich integriert wären.

Die DSGVO stellt mit privacy by design und by default zwar Grundsätze auf, die sich faktisch an die Hersteller richten, nimmt diese aber nicht als Verantwortliche in die Pflicht.

Bereits während der Produktentwicklung müssen Aspekte wie die Anwenderfreundlichkeit und der Schutz personenbezogener Daten in die Produktentwicklung einfließen. Deshalb ist es notwendig, nicht nur diejenigen Unternehmen und Behörden in die Verantwortung zu nehmen, die bestimmte IT-Produkte und -Verfahren einsetzen. Es müssen auch deren Hersteller in die Pflicht genommen werden.

Zudem sollten auf EU-Ebene einheitliche Bildsymbole – Piktogramme – zu den wesentlichen Merkmalen digitaler Produkte und Anwendungen erarbeitet werden. Mit diesen sollten die digitale Anwendungen und Produkte verpflichtend gekennzeichnet werden.

Beispiele für die Merkmale, die diese Symbole vermitteln sollen, sind:

- „Basisfunktionen nur mit Internetverbindung“
- „Nutzerdaten werden übermittelt“ oder
- „Nutzer-Tracking“.

Die Piktogramme würden es Käuferinnen und Käufern erlauben, sich einen schnellen Überblick über mögliche Datenschutzrisiken zu ver-

schaffen. Das könnte in die Kauf- bzw. Beschaffungsentscheidung einfließen.

d. Transparenz schafft Vertrauen

Systeminterne und selbstständige Verfahren der technischen Entscheidungsfindung begegnen vielen Ängsten und Vorbehalten. Es gibt Einsatzszenarien künstlicher Intelligenz, bei denen die negativen Befürchtungen berechtigt sind: Beispielsweise das Social Scoring in China oder Predicitive Policing, also die vorhersagende Polizeiarbeit.

Die Datennutzungen sind heute so komplex und umfassend geworden, dass der Einzelne häufig nicht mehr in der Lage ist, den Überblick über die Verwendung seiner Daten zu behalten. Datenschutzhinweise werden nicht gelesen, stattdessen wird mit einem Klick das Einverständnis erteilt. Mancher Bürger – gerade der älteren Generation – wählt den entgegengesetzten Weg und verzichtet aus Angst vor Datenmissbrauch ganz auf die digitale Teilhabe.

Keines von beidem kann die Lösung sein. Weder **digitaler Fatalismus** noch **digitale Askese**. Transparenzpflichten und klare Grenzen für das Erlaubte sollten den Bürgerinnen und Bürgern ihre digitale Selbstbestimmung zurückgegeben.

Hier könnte das eingangs genannte **Bürgerportal** weiterhelfen. Es könnte den Bürgerinnen und Bürgern eine erleichterte Möglichkeit bieten, ihre Datenschutzrechte wie das Recht auf Auskunft oder Berichtigung über eine zentrale Plattform auszuüben. Auch sollten die

Bürgerinnen und Bürgern die Möglichkeit haben, ihre Datenspuren nachzuverfolgen. Denkbar wären hier neue Ansätze, bei denen die Menschen ihr Recht auf Auskunft nicht aktiv einfordern müssen, sondern über eine zentrale Plattform Einsicht in die bei den jeweiligen Behörden gespeicherten und von diesen an Dritte übermittelten Daten erhalten. Alle Möglichkeiten, die Kontrolle und Übersicht über die eigenen personenbezogenen Daten zurückzugewinnen, sollten von der Verwaltung zum Nutzen der Bürgerinnen und Bürger ausgeschöpft werden.

VII. Fazit

Ich komme nun zum Schluss und möchte noch einmal betonen, dass unsere grundlegenden Werte, Rechte und Freiheiten durch digitale Technologien nicht beschnitten werden dürfen. Die Digitalisierung ist kein Selbstzweck. Sie soll dem Menschen dienen und muss der Demokratie verpflichtet sein. **Digitale Technologien müssen den Grundsätzen der Selbstbestimmung und der Privatheit, der Sicherheit und der Nachhaltigkeit genügen.** Nur wenn die Menschen darauf vertrauen können, werden sie den digitalen Wandel als Chance sehen und mitgehen.

Als Deutsche und als Europäer wollen wir eine Digitalisierung, die unsere Werte widerspiegelt und mit der wir in den wissenschaftlichen, technologischen, gesellschaftlichen und wirtschaftlichen Wettbewerb eintreten. Wir Datenschützer haben die Verantwortung dafür zu sorgen, dass dabei die Grundrechte garantiert werden.

Ich danke Ihnen für Ihre Aufmerksamkeit.