Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Vortrag

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Ulrich Kelber

„Alle meine Daten – der Abschlussbericht der Datenethikkommission“

bei Hochschule Bonn-Rhein-Sieg

Sankt Augustin, den 4. November 2019

Es gilt das gesprochene Wort

Einleitung

Die Datenethikkommission hat am 23. Oktober ihr Abschlussgutachten an die Bundesregierung übergeben.

Die DEK betont in ihrem Gutachten die herausragende Rolle des Datenschutzes im digitalen Zeitalter und gibt eine Reihe zukunftsweisender Handlungsempfehlungen, zum Datenschutz und zur Datennutzung.

Seit meiner Ernennung zum Bundesbeauftragten für den Datenschutz und die Informationsfreiheit im Januar bin ich Mitglied der DEK und habe die Sichtweise des Datenschutzes in die Beratungen eingebracht.

Voßhoff

Team

Die Datenethikkommission

Lassen Sie mich mit ein paar Sätzen zur Datenethikkommission selbst beginnen:

Die DEK wurde im Juli letzten Jahres von der Bundesregierung eingesetzt, um sich mit den Leitfragen zu den Themenkomplexen Algorithmische Prognose- und Entscheidungsprozesse, Künstliche Intelligenz und Daten auseinanderzusetzen.

Die 16 Mitglieder stammen aus Wissenschaft, Wirtschaft, Verbraucher- und Datenschutz.

Den inhaltlichen Rahmen für die DEK hatte die Bundesregierung mit einem Fragenkatalog vorgegeben. Die DEK sollte danach „Leitlinien für den Schutz des Einzelnen, die Wahrung des gesellschaftlichen Zusammenlebens und die Sicherung und Förderung des Wohlstandes im Informationszeitalter entwickeln.“ Zudem sollten Handlungsempfehlungen erarbeitet werden, wie diese „ethischen Leitlinien entwickelt, beachtet, implementiert und beaufsichtigt werden können“.

Diese Fragen hätten Arbeit für fünf bis zehn Jahre geboten, Vorgabe war aber ein Jahr.

Die DEK kam ab September 2018 jeden Monat zu einer zweitägigen Sitzung zusammen.

In der interdisziplinären Kommission wurden die Herausforderungen der Digitalisierung aus den unterschiedlichsten Blickwinkeln betrachtet und diskutiert. Es gab Plädoyers für Forschungsfreiheit in der Medizin und solche für den Schutz der Patientendaten. „Kämpfer“ für die Digitalisierung in der Wirtschaft und „Beschützer“ der Beschäftigten.

Dennoch waren die Diskussionen durchweg durch eine sachliche Arbeitsatmosphäre, gegenseitigen Respekt und die Bereitschaft zu Kompromissen gekennzeichnet.

Auf den Sitzungen wurde ausgiebig und lange – gegen Ende auch bis in den späten Abend hinein – diskutiert. Und auch zwischen den Sitzungen arbeiteten die Mitglieder mit Hochdruck an den Fragestellungen. Und nach und nach entstand das Abschlussgutachten der DEK.

Dieses kann sich auch aus Sicht des Datenschutzes sehen lassen.

Die DEK hebt in ihrem Gutachten nicht nur die abstrakte Wichtigkeit des informationellen Selbstbestimmungsrechts des Einzelnen hervor, sondern gibt konkrete Handlungsempfehlungen, wie diese Selbstbestimmung besser in die digitale Entwicklung integriert werden kann, um einen werteorientierten Fortschritt sicherzustellen.

Bedeutung von Daten- und Grundrechtsschutz für die digitale Zukunft

Für mich als Bundesbeauftragter für den Datenschutz war von Anfang an klar, dass eine ethische und gerechte Datenpolitik nur mit einem starken Datenschutz denkbar ist.

Die DEK ergreift hier klar Position, unterstützt die bewährten Grundprinzipien des Datenschutzes und spricht sich an entscheidenden Stellen für eine Nachschärfung des Datenschutzes aus.

Wie zu erwarten, hat dies zu Reaktionen bei wirtschaftsnahen Medien geführt, die zum Teil davon sprachen, dass eine „neue Datenregulierungswelle“ anrolle. Dabei ist es ein Irrglaube, dass es der Digitalisierung helfe, möglichst wenig zu regulieren und bestehende Regulierungen weitestgehend abzuschaffen.

Regulierung ist kein Selbstzweck. Sie dient letztendlich dazu, die Werte unserer Rechtsordnung zu gewährleisten und Grundrechte zu schützen.

Regulierung sollte insbesondere dort ansetzen, wo die Gefahren für die Rechtsgüter besonders hoch sind.

Dieser Anspruch von Regulierung ist auch nicht neu. Spätestens seit dem 19. Jahrhundert wurde technologische Entwicklung immer auch durch einen Rechtsrahmen flankiert, um etwa die Allgemeinheit vor bestimmten Risiken zu schützen. Die Erfolge dabei sind unbestreitbar, von der Sicherheit der Produkte bis hin zu den Fortschritten im Arbeitsschutz.

auch damals immer gegeben wird

Die Regulierung der Digitalisierung betrifft nicht nur das informationelle Selbstbestimmungsrecht und den Datenschutz.

Da die Digitalisierung nach und nach alle Lebensbereiche durchdringt, bestehen auch Auswirkungen auf ganz andere Rechtsgüter, wie die Gesundheit, die Berufsfreiheit oder das Rechts auf Gleichbehandlung. Denken wir beispielsweise an Künstliche Intelligenz in der Gesundheitsforschung, Pflegeroboter, automatisierte Bewerbungsverfahren oder die Risiken der Diskriminierung durch schlechte Datensätze.

Die DEK spricht sich daher an den Stellen für Regulierung aus, 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.

Transparenz

In meinem Vortrag wird es mir angesichts der Zeit und weil die Möglichkeit für eine Diskussion lassen möchte, nicht möglich sein, auf alle Aspekte des Abschlussgutachtens einzugehen. Ich möchte mich daher auf die Bereiche konzentrieren, die einen herausgehobenen datenschutzrechtlichen Bezug haben.

Ein Leitgedanke, der sich durch das Abschlussgutachten zieht und mir besonders am Herzen liegt, ist das Thema *Transparenz*.

Transparenz spielt aus datenschutzrechtlicher Perspektive eine große Rolle. Denn nur wenn der Einzelne ausreichend informiert wird, kann er sein informationelles Selbstbestimmungsrecht und seine daraus abgeleiteten Datenschutzrechte wahrnehmen. Nur wenn ich weiß, welche meiner Daten gesammelt werde, wozu diese genutzt werden und an wen sie weitergegeben werden, bin ich in der Lage eine informierte Einwilligung abzugeben. Nur wenn ich weiß, wer meine Daten nutzt kann ich meine Rechte auf Auskunft, Berichtigung oder Löschung geltend machen.

Die Datennutzungen sind heute so komplex und umfassend geworden, dass der Einzelne häufig nicht mehr in der Lage ist, einen Überblick über die Nutzung seiner Daten zu gewinnen und viele es lieber gar nicht mehr versuchen und „aufgeben“.

Dies geschieht entweder, indem Datenschutzhinweise einfach gar nicht gelesen werden bzw. zu allem ein Einverständnis erteilt wird oder mancher Bürger – gerade der älteren Generation, aber auch die besonders aufgeklärten Teile der Bevölkerung – aus Angst vor Datenmissbrauch ganz auf digitale Teilhabe oder bestimmte digitale Dienstleistungen verzichtet.

Beides kann nicht die Lösung sein. Vielmehr sollte unter anderem durch gezielte Transparenzpflichten den Bürgerinnen und Bürgern die Herrschaft über ihre Daten zurückgegeben werden.

Die DEK formuliert daher den ethischen Grundsatz der *interessenadäquaten Transparenz*:

„Derjenige, der Daten als Verantwortlicher verarbeitet, muss bereit und in der Lage sein, darüber Rechenschaft abzulegen. Dies erfordert ein angemessenes Maß an Transparenz und Dokumentation des Handelns und gegebenenfalls auch entsprechende Haftungsregelungen.“

Die Anwendung dieses Grundsatzes führt dann bei verschiedenen Handlungsempfehlungen zur Stärkung der Transparenz, von denen ich nur einige exemplarisch nennen möchte:

- Profilbildung und Scoring

Als erstes möchte ich die Forderung der DEK nach mehr Transparenz bei Profilbildungen ansprechen. Im Bereich von Profilbildung und insbesondere beim Scoring fordert meine Behörde schon seit Jahren mehr Transparenz. Dieser Forderung hat sich nun auch die DEK angeschlossen. Die DEK fordert „spezifische Kennzeichnungs-, Informations- und Auskunftspflichten bezüglich der Profilbildungen als solcher“. Die Informationspflichten sollen nicht nur bei automatisierten Entscheidungen greifen, sondern allgemein beim Einsatz von Algorithmen zur Profilbildung. Denn die Verknüpfung erhobener Daten und die Ableitung von Erkenntnissen aus diesen Daten machen zunehmend die Datenwirtschaft aus.

Hiermit verbunden fordert die DEK auch ein Recht auf einen „digitalen Neuanfang“ durch Löschung der gebildeten Profile, z. B. mit Erreichen der Volljährigkeit.

- Piktogramme für Produkte und Dienstleistungen

Ein anderes Beispiel ist das datenschutzfreundliche Design von Produkten und Dienstleistungen.

Die DEK empfiehlt verbindliche Vorgaben für datenschutzfreundliches Design von Produkten und Dienstleistungen, insbesondere wenn sich diese an Verbraucher richten. In diesem Zusammenhang fordert die DEK auch einheitliche Bildsymbole (sogenannte Piktogramme) einzuführen, die dem Verbraucher eine informierte Kaufentscheidung ermöglichen sollen.

Ein Verbraucher könnte dann mit einem Blick beispielsweise erkennen, ob ein Gerät personenbezogene Daten durch Sensoren wie Kamera oder Mikrofone erfasst und ob diese via Internet an den Hersteller übermittelt werden.

- Kennzeichnung von Bots

Als dritte Transparenzforderung möchte ich noch die Kennzeichnungspflicht für Social Bots nennen. Dabei kenne ich die Debatte, ob Social Bots wirklich schon ein relevantes Problem sind. Die technische Basis dafür ist aber auf jeden Fall vorhanden.

Die Authentizität zwischenmenschlicher Kommunikation ist nach Ansicht der DEK Grundbedingung für einen vertrauensvollen Umgang miteinander in der Gesellschaft.

Daher sollten Social Bots, sobald eine Verwechselungsgefahr zwischen Mensch und Maschine besteht, gekennzeichnet werden.

Besonders akut ist die Kennzeichnungspflicht im Bereich sozialer Netzwerke und anderer Medienintermediäre. Hier besteht eine Gefahr für den demokratischen Prozess, indem durch Social Bots versucht wird, Einfluss auf die öffentliche Meinungsbildung zu nehmen.

Transparenz ist damit der Anfang eines ethischen Umgangs mit Daten, aber nicht das alleinige Prinzip. Absolute Regeln, technische Lösungen ergänzen das Transparenzprinzip.

Algorithmische Systeme

Einen Schwerpunkt bilden auch die Handlungsempfehlungen der DEK zu Algorithmischen Systemen.

Hierzu möchte ich kurz darauf eingehen, warum die DEK ihre Handlungsempfehlungen auf Algorithmische Systeme als solche bezieht und nicht zwischen Künstlicher Intelligenz und „normalen“ Algorithmen unterscheidet. Der Fokus liegt in der öffentlichen Debatte stark auf dem Einsatz Künstlicher Intelligenz und dem Maschinellen Lernen.

Doch die ethischen Fragestellungen für den Einsatz von Algorithmen stellen sich ebenso bei normalen „klassischen“ Algorithmen.

Daher macht die DEK in ihren Handlungsempfehlungen generell keine Unterscheidungen zwischen der Art des Algorithmus, sondern spricht allgemein von algorithmischen Systemen.

- Risikoadaptierter Regulierungsansatz

Die Datenethikkommission hat - Sie werden es schon geahnt haben - auch für den Einsatz algorithmischer Systeme einen risikoadaptierten Regulierungsansatz gewählt.

Künftige Regulierung soll sich am Schädigungspotenzial des algorithmischen Systems ausrichten. Bei der Beurteilung des Schädigungspotentials kommt es „auf das gesamte sozio-technische System an“. Das bedeutet, dass alle Komponenten einer algorithmischen Anwendung, einschließlich aller beteiligten menschlichen Akteure bei der Bewertung berücksichtigt werden müssen.

Wie Kritiker darin ernsthaft einen „Generalverdacht“ gegen Algorithmen sehen können, ist mir schleierhaft.

- Kritikalitätsstufen

Die DEK empfiehlt, ein übergreifendes Modell zu entwickeln, nach dem algorithmische Systeme aus Sicht der Regulierung Kritikalitätsstufen zugeordnet werden.

Die DEK empfiehlt dabei fünf Kritikalitätsstufen.

Auf Stufe 1 stünden Anwendungen ohne oder mit geringem Schädigungspotenzial. Hier würde es weder spezieller Qualitätsanforderungen noch besonderer Kontrollmechanismen bedürfen. Als Beispiel nennt die DEK den in einem Getränkeautomaten eingesetzten Algorithmus.

Es ist dabei offensichtlich, dass die weit überwiegende Zahl aller Algorithmen dieser Stufe angehören und keinerlei spezifische Verpflichtungen für die Entwicklerinnen und Entwickler auslösen.

Auf Stufe 2 stehen Anwendungen mit einem gewissen Schädigungspotenzial. Hier sollen erste Regulierungen greifen, wie etwa Ex-post-Kontrollen bei dem begründeten Verdacht eines Fehlverhaltens des Systems, die Veröffentlichung angemessener Risikofolgeabschätzungen oder branchenspezifische, von den Aufsichtsbehörden genehmigte Codes of Conduct mit zertifizierten Entwicklungsprozessen inklusive Qualitätstests, gerade auch der Trainingsdaten. Als Beispiel nennt die DEK dynamische Preissetzungen ohne Personalisierung.

Bei regelmäßigem oder deutlichem Schädigungspotenzial (Stufe 3) sollten zusätzlich für spezifische Fälle Zulassungsverfahren vorgesehen werden. Ein möglicher Anwendungsfall sind personalisierte Preise.

Stufe 4 betrifft Anwendungen mit erheblichem Schädigungspotential. Hier fordert die DEK zusätzlich weitergehende Kontrollmöglichkeiten wie beispielsweise die Möglichkeit der kontinuierlichen behördlichen Kontrolle über eine Live-Schnittstelle. Möglicher Anwendungsfall ist die Beurteilung der Kreditwürdigkeit durch Akteure mit massiver Marktmacht.

Stufe 5 beträfe Anwendungen mit einem unvertretbaren Schädigungspotenzial, die zu verbieten wären. Beispiel hierfür wären algorithmendeterminierte Tötungen durch den Einsatz von autonomen Waffensystemen. Diese sind von der bloßen Unterstützung bei der Objekterkennung u.ä. Methoden sauber zu unterscheiden.

Um das skizzierte Regulierungsmodell umzusetzen, empfiehlt die DEK der Bundesregierung auf eine horizontale Algorithmen-Verordnung auf EU-Ebene hinzuwirken.

Eine europäische Verordnung sollte die zentralen Grundprinzipien für algorithmische Systeme enthalten. Wichtig sind dabei unter anderem Regelungen zur Zulässigkeit und Gestaltung algorithmischer Systeme, zu Transparenz und zu Betroffenenrechten.

Diese sollte dann durch sektorspezifische Regelungen je nach Zuständigkeit auf EU oder Bundesebene ergänzt werden.

Klare Regelungen sind dabei auch im Sinne der Entwicklerinnen und Entwickler, die Rechtssicherheit haben und auf dem Markt ein level playing field vorfinden, wenn die EU sich bei der Regulierung wieder auf ein Marktortprinzip einigen kann.

Innovative Datenmanagementsysteme

Neben dem Gesichtspunkt der Transparenz und der Kontrolle algorithmischer Systeme möchte ich auf einen dritten Aspekt des Abschlussgutachtens eingehen. Dieser betrifft die Förderung innovativer Datenmanagement- und Datentreuhandsystemen.

In der öffentlichen Debatte werden Digitalisierung und Datenschutz oft als unvereinbare Gegensätze dargestellt. Dass dies nicht der Fall ist, sondern digitale Innovationen vielmehr auch einen wichtigen Beitrag zur Stärkung des Datenschutzes leisten können, zeigt dieser Aspekt.

Unter Datenmanagement- und Datentreuhandsystemen werden verschiedenste Modelle verstanden. Zu den Privacy Management Tools (PMT) werden Anwendungen zur vereinfachten Einwilligungsverwaltung gezählt, wie beispielsweise Dashboards aber auch KI-Tools, die individuelle Nutzerpräferenzen automatisch umsetzen (sog. „Datenagenten“). Diese würden – neben einer Cookie-Diät der Anbieterinnen und Anbieter – auch gegen nervtötende Aufgaben wie Cookie-Banner & Co. helfen und damit mehr Datenschutz in der Praxis realisieren.

Daneben gibt es Personal Information Management Systems (PIMS). Bei ihnen stehen nicht die Herstellung und der Support technischer Anwendungen im Vordergrund, sondern die Dienstleistungen. Hier beginnt es bei Single-Sign-On-Diensten über lokale Datensafes und Online-Speichersysteme und reicht bis zu mehr oder weniger umfassender Fremdverwaltung der Daten der Nutzenden (sog. Datentreuhand-Modelle).

Gemeinsames Ziel ist die Befähigung des Einzelnen zur Kontrolle über seine personenbezogenen Daten sowie die Entlastung des Einzelnen von Entscheidungen, die ihn überfordern. Die DEK empfiehlt, Forschung und Entwicklung im Bereich von Datenmanagement- und Datentreuhandsystemen intensiv zu fördern.

Von PMT/PIMS können auch Gefahren ausgehen. Bei fehlerhafter Ausgestaltung von PMT/PIMS besteht die Gefahr, dass sich der Einsatz von PMT/PIMS in sein Gegenteil verkehrt. Statt echte Selbstbestimmung zu ermöglichen, könnten PMT/PIMS auch zur unbewussten oder sorglosen Fremdbestimmung eingesetzt werden.

PMT/PIMS sollen Hilfsmittel für die betroffenen Personen sein, dürfen ihre selbstbestimmte Entscheidung aber nicht vollständig ersetzen oder gar manipulieren. Ein missbräuchlicher Passwortsafe oder ein Datentreuhänder, der durch eine zu großzügige Überlassung von Daten seinen Gewinn steigern könnte, wären aus Sicht des Datenschutzes ein Albtraum.

Die DEK empfiehlt daher eine begleitende Regulierung von PMT/PIMS.

Es bedarf der Erarbeitung von Qualitätsstandards für PMT/PIMS sowie ein Zertifizierungs- und Überwachungssystems. Letzteres sollte insbesondere für Systeme greifen, die im Namen der betroffenen Personen agieren oder durch ihre technische Gestaltung die Entscheidungen der betroffenen Personen wesentlich steuern und kanalisieren.

Wir sehen darin auch ein attraktives Geschäftsfeld, gerade für deutsche Firmen, die wegen unserer strengeren Gesetze glaubwürdig auf dem Markt auftreten können. Vertrauen ist die Währung der Digitalisierung, dass vergessen manche Wirtschaftsverbände immer wieder leichtfertig.

Damit PMT/PIMS eine hinreichende Breitenwirkung erzielen können, sind sie auf die Kooperation aller betroffenen Verantwortlichen angewiesen. Die datenschutzrechtlichen Verantwortlichen sollten daher – unter sachgerechten Bedingungen – verpflichtet werden, die Kontrolle des Zugangs zu personenbezogenen Daten durch PMT/PIMS zu ermöglichen. Realistisch erscheint es hier sektorspezifisch vorzugehen und beispielsweise mit sozialen Netzwerken zu beginnen.

Zudem muss durch entsprechende gesetzliche Vorgaben sichergestellt werden, dass die Anbieter von PMT/PIMS stets im alleinigen Interesse der Betroffenen handeln und Unternehmen mit konfligierenden Interessen ausgeschlossen werden. Insbesondere dürfen sie kein Eigeninteresse an der Verwertung oder Weitergabe der Daten haben.

Werden diese Vorgaben eingehalten können PMT/PIMS die Funktion einer wichtigen Schnittstelle zwischen Belangen des Datenschutzes und der Datenwirtschaft zukommen.

Insbesondere erwartet die DEK durch Datentreuhänder auch einen Schub in der Nutzung von Daten für medizinische Forschung und andere gesellschaftliche relevante Prozesse wie z.B. Verkehrssteuerung.

In der DEK haben wir nämlich nicht nur den Datenschutz hochgehalten, sondern auch die Meinung vertreten, dass die Nichtnutzung von Daten auch unethisch sein kann.

Anonymisierung von Daten

Als vierten Aspekt möchte ich noch auf die Anonymisierung personenbezogener Daten eingehen.

Das Abschlussgutachten der DEK widmet sich nicht nur der Nutzung personenbezogener Daten, sondern auch dem Zugang zu und der Nutzung von nicht-personenbezogenen Daten.

In der Praxis besteht häufig das Problem, dass unklar ist, ob es sich bei einem Datensatz um eindeutig personenbezogene, pseudonymisierte oder anonyme Daten handelt. Je nachdem greifen unterschiedliche Rechtsvorschriften und es ist für Unternehmen aber auch für Forschende von enormer Bedeutung Klarheit darüber zu haben, wann sie mit personenbezogenen Daten arbeiten, und wann nicht. Ansonsten würden Firmen in Deutschland und Europa unnötig Nutzungsmöglichkeiten verwehrt.

Die DEK fordert daher die Entwicklung von Verfahren und Standards zur Anonymisierung von Daten zu intensivieren.

Um mehr Rechtssicherheit zu erreichen, sollten auf EU-Ebene handhabbare Standards zur Anonymisierung festgelegt werden. Damit verbunden sollten gewisse Vermutungsregelungen sein, die bei Einhaltung der Standards eingreifen.

Dabei sollte es den Datenschutzbehörden aber möglich bleiben, die Vermutung notfalls auch zu widerlegen, sollten die Standards von der technischen Realität überholt werden und eine Personenbeziehbarkeit wieder möglich werden.

Sinnvoll wäre es auch, die Standards aufgrund der weiter fortschreitenden technischen Entwicklungen von vornherein mit einer zeitlichen Gültigkeit zu versehen. Es macht ja einen Unterschied, ob anonymisierte Daten z.B. in der Netzsteuerung für wenige Stunden verwendet werden oder mit biologischen Material verbundene Daten für 30 Jahre gespeichert werden.

Zusätzlich sollten standardisierte Prüfmethoden entwickelt werden, um vermeintlich anonyme Datenbestände auf Personenbeziehbarkeit zu überprüfen.

Die DEK empfiehlt außerdem, eine Strafbarkeit für die Re-Personalisierung von anonymisierten oder pseudonymisierten Daten zu prüfen, auch wenn die Nachweisbarkeit davon sicherlich schwierig wäre.

Weitere Aspekte

Mit diesen Punkten habe ich Ihnen hoffentlich einen ersten Eindruck über das umfangreiche Abschlussgutachten der DEK vermitteln können. Weitere Handlungsempfehlungen, die ich nur kurz aufzählen, aber auf die ich an dieser Stelle leider aus Zeitgründen nicht näher eingehen kann sind:

- Der Vorschlag der DEK, in bestimmen Sektoren Anbieter zur Interoperabilität bzw. Interkonnektivität ihrer Anwendungen zu verpflichten. Diese Pflicht käme etwa bei Messenger-Diensten in Betracht und könnte den Markteintritt für neue, insbesondere auch europäische Anbieter, erleichtern.

- Der Vorschlag der DEK das Haftungsrecht bezogen auf den Einsatz von Algorithmen und digitalen Produkten anzupassen.

- Der ganze Bereich des Open Government Data. Die DEK vertritt hier die Auffassung, dass der öffentliche Sektor mehr (anonyme) Daten zur Verfügung stellen sollte und entsprechende Infrastrukturen ausgebaut werden sollten.

- Die DEK empfiehlt angesichts des technischen Fortschritts im Bereich KI, Stimmerkennung, Sensoren und Videoüberwachung eindringlich einer Verbesserung des Datenschutzes für Beschäftigte und insbesondere auch Bewerberinnen und Bewerber.

- Als letzten Punkt möchte ich noch erwähnen, dass die DEK sich nicht nur mit dem Schutz personenbezogener Daten des Einzelnen beschäftigt, sondern sich auch für eine Verbesserung des Schutzes der Daten von Unternehmen ausspricht.

Fazit

Die Datenethikkommission hat mit ihrem über 200 Seiten starkem Abschlussbericht ein umfangreiches Gutachten vorgelegt.

Das Papier enthält insgesamt 75 Handlungsempfehlungen.

Die DEK hat sich dabei nicht auf allgemeine Forderungen und hehre Ziele beschränkt, sondern versucht der Bundesregierung und damit der Öffentlichkeit möglichst konkrete Handlungsempfehlungen an die Hand zu geben.

Diese können nicht in allen Fällen durch die Bundesregierung alleine umgesetzt werden. Insbesondere im Bereich datenschutzrechtlicher Regulierung ist ein Tätigwerden auf EU-Ebene gefordert.

Die Bundesregierung kann hier jedoch wichtige Impulse setzten und sich für entsprechende Regulierungsmaßnahmen einsetzten. Eine große Chance bietet hier die anstehende deutsche EU-Ratspräsidentschaft im zweiten Halbjahr 2020.

Wie Sie sich vorstellen können, werde ich mir nicht nehmen lassen, die Bundesregierung - bei sich bietenden Gelegenheiten oder auch unabhängig davon - an die Handlungsempfehlungen der Datenethikkommission zu erinnern.

Ich freue mich nun auf die Diskussion und danke Ihnen für Ihre Aufmerksamkeit.