Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Key Note

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Ulrich Kelber

„1 Jahr DSGVO – was ist, was kommt, was fehlt noch“

21. Jahresfachkonferenz

DuD 2019

Datenschutz und Datensicherheit

Ein Jahr DSGVO - erste Erfahrungen

3. Juni 2019 in Berlin

im Pullman Hotel Schweizerhof Berlin

Beginn: 8.00 Uhr

Redezeit: 8.45 Uhr – 9.15 UHR

Es gilt das gesprochene Wort

Sehr geehrte Frau Geuhs,

sehr geehrte Frau Dr. Mester,

liebe Kolleginnen und Kollegen,

geehrte Damen und Herren,

,

I. Vorbemerkung

Sie haben eine thematisch dichte und anspruchsvolle Tagung vor sich.

Ich danke für die Gelegenheit, hier in diesem Rahmen über ein Jahr DSGVO zu sprechen.

Diese seit 1994 stattfindenden Fachkonferenzen haben stets wichtig Impulse im Bereich Informationssicherheit und Daten-schutz gegeben.

Sie schreiben auf Ihrer Webseite, wie wichtig Ihnen die „hohe Qualität der Vorträge“ ist. Ich hoffe sehr, diesen Ansprüchen und Erwartungen zu genügen.

Und sollten Sie sich über mich ärgern: Dann bitte als Ergebnis einer (ich darf zitieren) „gemeinsamen, interaktiven und fachlich fundierten Kommunikation“, für die diese Tagung von jeher steht.

Ich jedenfalls freue mich auf den Austausch mit den hier vertretenen Fachleuten aus sehr unterschiedlichen Bereichen, von der Geschäftsleitung verschiedener Unternehmen bis hin zu den Anbietern und Betreibern von Sicherheitskonzepten.

Gespannt bin ich auf den Austausch mit Amtsleitern und Praktikern des Datenschutzes aus Ländern, Gemeinden und dem Bund.

Gerne nehme ich auch die Gelegenheit wahr, Kolleginnen und Kollegen aus den Datenschutz-Aufsichtsbehörden der Länder hier zu treffen.

Noch keine abschließende Bilanz der DSGVO

Nach gerade mal einem Jahr lässt sich noch kein abschließendes Gesamturteil über die neue Gesetzeslage fällen.

Inwieweit insbesondere die Harmonisierung des Datenschutzes und ein effektiver Schutz gegen Datenschutzverstöße erreicht worden ist, lässt sich noch nicht seriös bewerten.

An bestimmten Punkten lässt sich aber doch bereits erkennen, was erreicht wurde, wohin die Reise des Datenschutzes in den kommenden Jahren gehen könnte und welche Herausforderungen wir auf diesem Weg zu bewältigen haben werden.

Lassen Sie mich aber trotzdem ganz am Anfang ein Ergebnis meiner Ausführungen bereits vorwegnehmen:

Die DSGVO ist trotz einiger Schwächen und Lücken ein gelungener Wurf, um das europäische Datenschutzrecht nachhaltig zu verbessern.

Sie kann auch dazu beitragen, bestehende Lücken in Gesetzgebung und Vollzug zu schließen.

Sie ist ein Exportschlager!

II. Erste Ergebnisse der DSGVO

Seit einem Jahr gilt in der Europäischen Union ein für alle verbindliches Datenschutzgesetz. Sie beendet die alte Kleinstaaterei und setzt konsequent die Vorgaben der EU-Grundrechtecharta und der Europäischen Menschenrechtskonvention um. Sie gilt für öffentliche wie auch für nicht-öffentliche Stellen.

Fangen wir zunächst mit dem eher wenig Erfreulichen an: **Der Start der europäischen Grundverordnung war von allerlei Widrigkeiten und schlechter Presse begleitet.**

Fest steht: Viele Beteiligte waren trotz einer zweijährigen Übergangszeit schlecht auf die Umstellung vorbereitet. Noch im Herbst 2017 waren der Hälfte der Unternehmen in Deutschland die Regelungen der DSGVO nicht – oder noch nicht – bekannt.

Der Stolperstart lag aber auch der Stimmungsmache gegen die DSGVO. Vor allem mit dem Totschlagargument der angeblichen Überbürokratisierung wurden auch glatte Fehlinformationen unter die Leute gebracht.

Gezielte Angstmache und erhebliche Verunsicherung wurden in Vereine, und Startups hineingetragen, durchaus auch in der Hoffnung, teure Beratungsmandate zu erhalten. Selbst Privatleuten wurde in düsteren Farben eine Abmahnwelle größten Ausmaßes vorhergesagt. Da kann ich nur sagen: in meiner Behörde gingen gerade einmal 5 Beschwerden über Abmahnungen ein.

Die Zeitungen waren voll von Horrorgeschichten über weinende Lehrkörper, denen das Fotografieren ihrer Schutzbefohlenen bei Strafe des wirtschaftlichen Ruins verleidet werden sollte. **Auch hier: heiße Luft ohne rechtliche Substanz. In Wirklichkeit hat die DSGVO an der bestehenden Rechtslage kaum etwas verändert.**

Den Aufsichtsbehörden wiederum wurde unterstellt, nichts anderes im Schilde zu führen, als kleine Selbständige und Vereinsvorsitze mit Bußgeldern zu überziehen. Auch hier haben sich viele dieser Besorgnisse natürlich als unbegründet erwiesen. Die Aufsichtsbehörden haben gerade bei kleinen und mittleren Unternehmen, Vereinen und Privatleuten eben gerade nicht mit der großen Keule zugeschlagen. Sie haben vielmehr durch Beratung geholfen, an vielen Stellen die vorhandenen Startschwierigkeiten zu überwinden.

Der Kollege Dr. Brink aus Baden-Württemberg wird im Anschluss an meine Keynote die Bußgeldpraxis näher erläutern. Er wird anschaulich darlegen können, dass die Datenschutz-Aufsichtsbehörden alles andere sind als mobile Inkassobüros.

Lassen Sie mich bei dieser Gelegenheit den Kolleginnen und Kollegen aus den Ländern meine persönliche Anerkennung für ihre enormen Kraftanstrengungen bei der Umsetzung der DSGVO aussprechen.

Neben Dr. Brink sind auch noch weitere Kolleginnen und Kollegen hier auf diesem Kongress.

Gerade die Datenschutzaufsichtsbehörden der Länder – sie sind für den allergrößten Teil des Datenschutzes in der Privatwirtschaft zuständig – haben mit oftmals viel zu wenig Personal und bedenklich knappen Ressourcen die schwierige und zeitaufwendige Informationsarbeit geleistet. Ich bin sicher, sie werden das auch gemeinsam mit meiner Behörde in der Datenschutzkonferenz auch weiterhin tun.

Viele Fragen aus der Mitte der Gesellschaft konnten durch diese intensive Aufklärungsarbeit geklärt werden.

Gleiches gilt im Übrigen für die betrieblichen und behördlichen Datenschutzbeauftragten, die wertvolle Arbeit bei der Anpassung der Arbeitsprozesse in Betrieben und Behörden geleistet haben und weiterhin leisten werden. Ich warne Regierung und Parlament noch einmal davor, die bewährte Bestellungspflicht für betriebliche Datenschutzbeauftragte kurzsichtig aufzugeben. Machen Sie die Betriebe nicht blind, wenn es um die Erfüllung der gesetzlichen Verpflichtungen geht.

Mit der DSGVO ist der Datenschutz wieder stärker in das Bewusstsein der Bürgerinnen und Bürgerinnen gerückt.

In meinem Haus hat sich die Anzahl der Beschwerden über Datenschutzverstöße gegenüber Vor-DSGVO-Zeiten mehr als verdreifacht, von früher 400 Beschwerden und Anfragen pro Monat auf nun fast 1.400.

Die Bürgerinnen und Bürger berufen sich besonders auf ihre Betroffenenrechte, wie Datenauskunft und Datenlöschung.

Auch bei den Aufsichtsbehörden der Länder haben die **Beschwerden, allgemeinen Anfragen und Meldungen von Datenschutzverstößen** erheblich zugenommen.

Datenschutz als Wettbewerbsvorteil

Zu den unbestreitbaren Vorzügen der DSGVO gegenüber der alten Richtlinie aus dem fernen Jahr 1995 gehören vor allem die erweiterten Betroffenenrechte – wie etwa das Recht auf Datenübertragbarkeit oder das ***Recht auf Vergessenwerden*** – ebenso wie die Verpflichtungen, die Datenverarbeitung datenschutzfreundlich zu gestalten („***Privacy by Design“ und „Privacy by Default“).***

Lassen Sie mich diese in der öffentlichen Diskussion stark vernachlässigte Regelung in ihrer praktischen Bedeutung hervorheben. Die Grundverordnung eröffnet hier der europäischen Digitalwirtschaft eine große Chance. **IT-Verfahren- und Produkte „made in Europe“ sind ein Erfolgsmodell im internationalen Wettbewerb!**

Privacy by Design“ und „Privacy by Default bringen einen entscheidende Vorteil auch für die europäische Digitalwirtschaft, den es zu nutzen gilt. Auch die Datenschutz-Aufsichtsbehörden sollten IT-Verfahren und Produkten „**made in Europe**“ unter die Arme greifen, und gemeinsam eine vertrauenswürdige – und das heißt am Datenschutz ausgerichtete - Digitalisierung auf die Beine stellen.

Gerade kleine und mittlere Unternehmen sollten die Gelegenheit beim Schopfe fassen, mit datenschutzfreundlichen Produkten und Anwendungen auf den Märkten zu punkten. Gelingt es – auch mit Hilfe der Datenschutz-Aufsichtsbehörden – europäische Produkte schon mit der Entwicklung der Produkte so datenschutzfreundlich auszurichten, werden diese Unternehmen auf den internationalen Märkten einen Wettbewerbsvorteil erreichen.

Raus aus dem Jammermodus, rein in den Wettbewerb. Die Automobilkonzerne haben sich doch früher auch nicht endlos im Kampf gegen die Anschnallpflicht verloren, sondern den Airbag beworben. Gerade auch in den USA, wo es so etwas noch nicht gab. Wo ist die Werbung für IT-Produkte und IT-Dienstleistungen aus Europa, bei deren Nutzung man glaubhaft nicht mit seiner persönlichen Daten und damit dem Verlust seiner Privatsphäre bezahlen muss? Fällt den deutschen Wirtschaftsverbänden denn wirklich nicht auf, dass auch hier droht, von den USA überholt zu werden?

Ein weiterer ökonomischer Vorteil: Durch die DSGVO haben es Unternehmen ebenso wie Bürgerinnen und Bürger bei den Aufsichtsbehörden jeweils nur noch mit einem Ansprechpartner zu tun. Das ist vor allem für grenzüberschreitend tätige Unternehmen und die Verbraucher ein großer Vorteil.

Internationale Fortschritte durch die DSGVO

Die DSGVO hat sich mittlerweile allen Unkenrufen zum Trotz zu einem internationalen **Standard entwickelt. Daran orientieren sich auch andere Weltregionen.** Die Entwicklungen in Japan, Brasilien und Indien, aber auch das hohe Interesse weiterer Staaten in Lateinamerika und Asien belegen dies eindrucksvoll.

Anlass zum Optimismus gibt auch die Entwicklung des Datenschutzes in Kalifornien und den USA.

In Kalifornien wurde als **Reaktion auf den Facebook-Skandal nach dem expliziten Vorbild der DSGVO der "California Consumer Privacy Act" verabschiedet.** Unternehmen müssen ab dem 1. Januar 2020 offenlegen, welche Kunden- und Nutzerdaten sie speichern. Die Nutzer wiederum erhalten das Recht, die Verwendung ihrer persönlichen Daten zu kommerziellen Zwecken zu unterbinden. Die Internetfirmen werden verpflichtet, einen Link anzubieten, der es den Nutzern erlaubt, ohne Papierkrieg den Weiterverkauf ihrer Daten verhindern.

Es sind zwar keine Zwangsmaßnahmen und keine Bußgelder vorgesehen, die Verbraucher können aber einfach gerichtlich ihre Rechte gegenüber den Unternehmen geltend machen.

Kalifornien ist der Sitz zahlreicher Technologiekonzerne, so dass dem neuen Gesetz eine wichtige Pilotfunktion zukommt.

In Washington D.C. reifen die Pläne, das kalifornische Gesetz als Vorbild für eine US-weite Regelung zu machen.

Die europäische Idee von Datenschutz setzt sich weltweit durch. Ein weiteres Argument, dass europäische Unternehmen die Chance zu datenschutzfreundlichen Produkten und Dienstleistungen jetzt ergreifen müssen, um ihren Vorsprung nicht zu verlieren.

Schutz der individuellen Rechte der Menschen weltweit

Ein weiterer Aspekt betrifft die Perspektive der Bürgerinnen und Bürger, nicht nur in der EU, sondern noch darüber hinaus.

Hier leistet die Grundverordnung ihren Beitrag, die Menschen vor einer Verletzung ihrer Privatsphäre eben nicht mehr nur vor dem allwissenden Staat, sondern gerade auch durch Unternehmen wie Amazon, Google, Microsoft und Facebook zu schützen.

Dass europäische Datenschutzrecht bekennt sich deutlicher als je zuvor dazu, dass der Datenschutz keine beliebige Variante der Digitalisierung ist. Er ist ein Grund- und Menschenrecht. Freiheits- und Persönlichkeitsrechte stehen immer im Mittelpunkt der Rechtsordnung!

Ich möchte darauf hinweisen, dass die DSGVO – ebenso wie das vorherige Recht – auch deshalb weit über die Grenzen der EU hinauswirkt, weil sie immer gilt, wenn Europäerinnen und Europäer betroffen sind und eine Übermittlung personenbezogener Daten in Länder außerhalb der EU bzw. des EWR weiterhin nur dann erlaubt ist, wenn beim Empfänger ein angemessenes Datenschutzniveau besteht.

III. Ist die DSGVO das Ende aller Weisheit?

Wenn ich die großen Fortschritte der Grundverordnung hervorhebe, bin ich mir natürlich bewusst, dass die DSGVO erkennbare Schwächen aufweist.

Schon bei anderer Gelegenheit habe ich einen Vergleich zum „Ewigen Landfrieden“ gezogen. Wie der Datenschutz 1495 eine revolutionäre Idee, die heute selbstverständlich ist. Man darf sein Recht nicht mehr mit Gewalt durchsetzen, sondern muss sich an staatliche Institutionen wenden. Die damals aufgebaut werden mussten. Kleine Adlige waren der Meinung, dass sollte nicht für sie gelten. Die Könige und Fürsten setzten sich zu Anfang noch darüber hinweg. Aber die Idee setzte sich immer mehr durch. Und das, obwohl er nur aus 12 Paragraphen bestand.

Der europäische Gesetzgeber war vorausschauend genug, den **Evaluierungsprozess der DSGVO** festzuschreiben.

Ich hoffe sehr, dass die aus diesem Prozess entwickelten Reformvorschläge, die den Datenschutz stärken sollen, nicht auf taube Ohren stoßen.

Es gilt, den Datenschutz an den Stellen zu verbessern, die noch nicht zufriedenstellend gelöst sind. Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länger befassen sich zurzeit intensiv mit der anstehenden Evaluierung, um der Europäischen Kommission Vorschläge vorzulegen.

Ich möchte hier die bereits angesprochene Verpflichtung zum Einsatz datenschutzfreundlicher Technologie herausgreifen.

Warum setzt diese erst bei den datenschutzrechtlich Verantwortlichen an, d. h. den Unternehmen oder Behörden, die die Technologie einsetzen?

Sie haben in manchen Fällen gar keine oder nur eine geringe Auswahl, welche IT sie verwenden. Oder auch nur wenig Kenntnisse über die Funktionsweise. Wäre es deshalb nicht eher zielführend, hier viel früher, nämlich bei den Herstellern von IT-Verfahren und -Produkten anzusetzen? Hierzu hatte es bereits bei den Verhandlungen zur DSGVO Vorschläge gegeben, die ich gern wieder aufgreifen würde.

Wenn wir über eine Evaluierung der Datenschutz-Grundverordnung reden, müssen wir auch die Herausforderungen und Probleme aufgreifen, die mit Scoring und Profiling verbunden sind.

Die Bildung von persönlichen Profilen und deren – kommerzielle und politische – Auswertung wird in Zukunft eine immer größere Bedeutung haben werden. Wir haben es mit einem der zentralen Themen unserer Zeit zu tun.

Die Werkzeuge der Datenverarbeitung ermöglichen das Anlegen, die Auswertung und Analyse ungeheurer Datenmengen aus verschiedensten Kontexten. Verbunden mit immer weiter verfeinerten Möglichkeiten des Einsatzes selbstlernender Mechanismen eröffnet dies vielfältige Möglichkeiten, Verhalten von Einzelnen (vermeintlich) vorherzusagen und ggf. zu steuern.

Obwohl diese Entwicklung diverse datenschutzrechtliche Grundprinzipien herausfordert – z. B. das Gebot der Datenminimierung oder die Zweckbindung – bleibt die DSGVO gerade in diesem Punkt vage und weitgehend auf dem Stand von 1995. Bei den Verhandlungen zur Schaffung der DSGVO war es nicht gelungen, die Bildung von Profilen und das Scoring einer modernen europäischen Regelung zuzuführen. Hier sollten wir die Evaluierung für einen neuen Anlauf nutzen.

Ob das neue europäische Datenschutzrecht auf längere Sicht den Erfolg haben wird, den wir uns alle wünschen, hängt auch davon ab, ob wir im Bereich **Algorithmen und Scoring** zu Rechtssicherheit und vernünftigen Lösungen kommen.

Wer da glaubt, es ginge lediglich um eine Art finanzielle Wasserstandsmeldung der Schufa, irrt gewaltig. Das zeigt ein Blick in andere Länder exemplarisch. So wird in China, aber nicht nur dort, derzeit intensiv mit sog. „Super-Scores“ experimentiert. Bis 2020 sollen im Reich der Mitte alle Bürgerinnen und Bürger einem Sozial-Kredit-Regime unterworfen werden. Dieser Score soll auch für Unternehmen gelten. Ziel ist eine umfassende Bewertung sozialer und politischer Verhaltensweisen. Braves und regimetreues Verhalten soll auf diese Weise belohnt, aber Widerborstigkeit mit Sanktionen belegt werden.

Eine solche Politik der Selektion in gute und böse Bürger, oder – von gleicher Dimension - ein Geschäftsmodell gläserner Kundern durch private Konzerne ist nicht allein ein Angriff auf personenbezogene Rechte Einzelner. Wir haben es vielmehr mit einem digitalen Großangriff auf die Struktur und das innere Gefüge von Staat und Gesellschaft zu tun!

Das Beispiel China zeigt, was an Missbrauch möglich ist. Wir müssen daher den gesamten Bereich **Scoring und Profiling** dringend und tiefgreifend unter die Lupe nehmen. Sonst besteht die Gefahr, dass Teilelemente von dem, was sich in China anbahnt, tröpfchenweise auch hierzulande durchdringen. Im privaten Sektor hat dies schon begonnen.

Daher kann sich Europa nicht im wohligen Schauer über die Zustände in anderen Ländern erheben. Hier ist die liberale Zivilgesellschaft im Kern ihres Selbstverständnisses herausgefordert, diese Form der Kontrolle des Einzelnen wirkungsvoll und energisch zu regulieren und zu kontrollieren.

An dieser Stelle möchte ich ein paar Eckpunkte für eine Verbesserung der gesetzlichen Regelungen anführen:

- Die in Art. 15 Abs. 1 lit. h DSGVO bereits angelegten Anforderungen an die Verständlichkeit score-basierter Prozesse für den durchschnittlichen Verbraucher sollten mit Leben erfüllt und auf gesetzlicher Ebene verbessert werden.

- Die Scoring-Anbieter – und das sind nicht nur die Auskunfteien – müssen ihre Transparenzpflichten bei der Darstellung ihrer score-basierten Entscheidungen deutlich erweitern. Die Verbraucherinnen und Verbraucher haben einen Anspruch darauf, dass ihnen der Score und seine Eigenschaften gegenüber den Aufsichtsbehörden offen gelegt wird. Der Hinweis auf Betriebs- und Geschäftsgeheimnisse darf die Kontrollen nicht blockieren. Wenn wir als Aufsichtsbehörden bis zu einem bestimmten Punkt sogar Regierungsstellen und Geheimdienste kontrollieren dürfen, sollten sich die verantwortlichen Aufsichtsbehörden der Länder weder von der Schufa noch einem anderen Anbieter die Tür weisen lassen, wenn sie deren Umgang mit Scores kontrollieren wollen.

- Die Verbraucher haben ein Recht zu wissen, wie die Scores zwischen verschiedenen Gruppen mit unterschiedlichen geschützten Merkmalen verteilt sind. Dieses Wissen ist eine Voraussetzung dafür, algorithmische Diskriminierungen zu erkennen und dagegen vorzugehen. Auch an diesem Punkt müssen die Aufsichtsbehörden gestärkt werden. Sonst laufen die Rechte der Betroffenen schnell ins Leere.

- Die Anbieter sollten insbesondere in sensiblen Bereichen gegenüber den Aufsichtsbehörden die Qualität ihrer Verfahren darlegen müssen. Das muss dann auch überprüfbar sein. Gleiches gilt auch für die Verbesserung der Datenqualität. Hier liegt noch Vieles im Argen.

Die hier genannten Aufgaben lassen sich nur bewältigen, wenn die Aufsichtsbehörden ausreichend hoch qualifiziertes Personal zur Verfügung haben. Eine Aufsicht ohne Augenhöhe ist keine wirksame Kontrolle, sondern Augenwischerei.

Auf der anderen Seite will ich aber auch nicht verhehlen, dass es vielleicht auch den einen oder anderen Punkt gibt, bei dem vor allem der mit der Umsetzung der DSGVO verbundene bürokratische Aufwand keinen datenschutzrechtlichen Mehrwert bringt.

Es ergibt keinen Sinn, Regelungen zu verteidigen, die nur Arbeit machen und dem Datenschutz nicht von Nutzen sind. Ich sehe es als Aufgabe der Aufsichtsbehörden an, an bestimmten Stellen Reformbedarf aufzuzeigen, ob in der eigenen Aufsichtstätigkeit oder in der Verordnung selbst.

Im Rahmen der vorgesehenen Evaluierung werden wir konkrete Vorschläge für eine Optimierung des geltenden Rechts vorlegen. Wo der Aufwand zum Selbstzweck wird, ohne für den Schutz der Daten etwas zu erreichen, sind Korrekturen angebracht.

Datenschutz ins Grundgesetz

Wir feiern in diesen Tagen das 70-jährige Bestehen unseres Grundgesetzes. Diese Verfassung ist eine Erfolgsgeschichte. Die früheren Anläufe für einen Verfassungsstaat blieben auf halbem Wege stehen, scheiterten an der militärischen Übermacht der monarchischen Obrigkeit oder gingen im Desaster der NS-Diktatur und des von ihr entfesselten Krieges unter.

Es war 1949 ein revolutionärer Schritt, die Grundrechte an den Anfang als verbindliche Leitlinien staatlichen Handelns an die Spitze der Verfassung zu stellen.

Diese Regeln für Bürger und Staat wurden in der Zwischenzeit vielfach verändert, dennoch hat sich an dieser Grundaussage nichts verändert – und das ist gut so!

Die Welt ist aber seit damals nicht stehen geblieben. Hätten die Väter und Mütter des Grundgesetzes über Internet, Soziale Netzwerke und Mobiltelefone verfügt, hätten sie mit Sicherheit den Schutz der Persönlichkeitsrechte in der Digitalen Welt unmittelbar mit in den Grundrechtekatalog aufgenommen.

Heute lässt sich der Datenschutz als breites Grundrecht aus der Rechtsprechung des Bundesverfassungsgerichts ableiten. Wegweisend ist das Volkszählungsurteil aus dem Jahr 1983, in dem das Gericht die „informationelle Selbstbestimmung“ aus dem allgemeinen Persönlichkeitsrecht entwickelte und auch verbindliche Kriterien zu dessen Schutz entwickelte, die bis heute ihre Aktualität bewahrt haben und immer wieder in der weiteren Rechtssprechung bestätigt wurden.

Mit großem Interesse habe ich die die Überlegungen meines Hamburger Kollegen, Prof. Caspar, den Datenschutz ins Grundgesetz aufzunehmen zur Kenntnis genommen. Ich würde eine Diskussion über diesen Vorschlag begrüßen. Sicherstellen müssten wir natürlich, dass eine Kodifizierung im Grundgesetz die breite Anwendung des Grundrechts als Folge der Rechtssprechung des Bundesverfassungsgerichts nicht einschränkt, sondern stärkt.

IV. Was kommt noch auf den Datenschutz zu?

Hauptziel der DSGVO ist es, Bürgerinnen und Bürger bei der Verarbeitung ihrer personenbezogener Daten zu schützen. Bei der ePrivacy-Verordnung geht es um den speziellen Schutz des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation.

Beide Verordnungen überschneiden sich vielfach in ihren Schutzzielen.

Eigentlich sollten beide Verordnungen zeitgleich in Kraft treten. Das hat nicht geklappt. Es hakt und klemmt heftig. Viele Anti-Datenschutz-Lobbyisten sind unterwegs.

Die eigentlich in der ePrivacy-VO geplanten **Vorschriften zum Tracking** dürfen aber nicht zu Lasten der Bürgerinnen und Bürger verwässert werden. So darf die Einwilligung in die mit der Setzung von Cookies verbundene Datenverarbeitung nicht zur Bedingung für die Nutzung eines Kommunikationsdienstes gemacht werden Ich setze mich für ein ausdrückliches Kopplungsverbot ein.

Es darf auch nicht zu Inhaltsfiltern und Vorratsdatenspeicherungen kommen, um damit unspezifisch bestimmte Straftaten zu verfolgen.

Künstliche Intelligenz

Mit den vielschichtigen Fragen der Künstliche Intelligenz (KI) und seiner ambivalenten Beziehung zum Datenschutz befasst sich die diesjährige Datenschutzkonferenz unter Vorsitz meines rheinland-pfälzischen Kollegen Professor Kugelmann schwerpunktmäßig und hat dazu die „Hambacher Erklärung“ veröffentlicht. Zudem ist Künstliche Intelligenz auch eines der bestimmenden Themen der Datenethikkommission, deren Mitglied ich bin.

KI-Systeme werden beispielsweise in der Medizin bereits eingesetzt. Schon heute sind neuronale Netze in der Lage, automatisch komplexe Tumorstrukturen zu erkennen. KI-Systeme können auch genutzt werden, um Depressionserkrankungen anhand des Verhaltens in sozialen Netzwerken oder anhand der Stimmmodulation beim Bedienen von Sprachassistenten zu erkennen. In den Händen von Ärzten kann dieses Wissen dem Wohl der Erkrankten dienen, **in den falschen Händen aber schrecklich missbraucht werden.**

Auch zur Bewertung von Bewerbungsunterlagen werden bereits ein KI-System eingesetzt, mit dem Ziel, frei von menschlichen Vorurteilen zu entscheiden. Das ist in dem folgenden Beispiel allerdings mächtig schiefgegangen. Ein Unternehmen hatte bislang überwiegend männliche Bewerber eingestellt und das KI-System mit deren erfolgreichen Bewerbungen trainiert. In der Folge bewertete das System Frauen entsprechend sehr viel schlechter, obwohl das Geschlecht weder vorgegebenes Bewertungskriterium war, noch dem System überhaupt bekannt war. Dieses Beispiel offenbart die Gefahr, dass in Trainingsdaten abgebildete Diskriminierungen nicht beseitigt, sondern vielmehr sogar verfestigt und pseudo-objektiviert werden.

Die Beispiele machen das vorhandene Gefahrenpotential deutlich. Mit KI-Systemen werden häufig personenbezogene Daten verarbeitet. Diese Verarbeitung birgt erhebliche Risiken für die Rechte und Freiheiten von Menschen. Sie zeigen darüber hinaus, wie unverzichtbar es ist, diese hoch dynamische Entwicklung politisch, gesellschaftlich und rechtlich zu begleiten und vor allem aktiv zu gestalten.

Datenschutz als nachsorgende Kontrolle käme hier viel zu spät. Das ist Ziel und Inhalt der "Hambacher Erklärung" der Datenschutzkonferenz (DSK). Die Aufsichtsbehörden des Bundes und der Länder haben in diesem Dokument sieben Anforderungen an Systeme der KI aufgestellt. Die Erklärung setzt sich für eine datenschutzfreundliche Technikgestaltung von KI ein und formuliert die entsprechenden Voraussetzungen, darunter Transparenz, Nachvollziehbarkeit und Korrigierbarkeit.

In meinem Haus bereiten wir gerade für den 24. September 2019 in Berlin ein Symposium vor zum Thema "*Datenschutzrechtliche Ansprüche an den Einsatz von KI*.

V. Schlussbemerkung

Bei der DSGVO sind wir bereits in der ersten Phase der Evaluierung angelangt. Das Kind hat die Krabbelphase hinter sich und erschließt sich nun immer besser laufend die Welt.

Bei der e-Privacy-Verordnung hakt es noch gewaltig. Ich bin aber zuversichtlich, dass ihre Verabschiedung eine grundlegende Weichenstellung sein wird für den Schutz personenbezogener Daten in der elektronischen Kommunikation bringen wird.

Auf dem Spiel steht nicht weniger als die Zukunft der digitalen Gesellschaft.

Deshalb müssen aus meiner Sicht vor allem beim Scoring und der Profilbildung die Rechte der Bürgerinnen und Bürger gestärkt werden.

Zudem muss die von der DSGVO vorgesehene Schaffung eines Datenschutzrechts für Beschäftigte umgesetzt werden.

Auf der anderen Seite sind Solche Informations- und Dokumentationspflichten zu überprüfen, wo der Aufwand für den Verantwortlichen, ganz gleich welche Größe – ohne für den Schutz der Daten etwas zu erreichen – nur zum Selbstzweck führt.

Letztlich müssen wir bei uns all den sehr unterschiedlichen Baustellen die Frage stellen: Wollen wir in einer Gesellschaft leben, in der jeder die Vorteile der digitalen Technik selbstbestimmt nutzen kann? Oder wollen wir es zulassen, dass jeder von uns unweigerlich zum Objekt der „Datensammelei“ verkommt, um auf diese Weise bestimmte Interessen zu bedienen?

Es ist jetzt an der Zeit, einen angemessenen Schutzstandard für die Vertraulichkeit der elektronischen Kommunikation in den nächsten Jahren und Jahrzehnten zu etablieren und die vorhandenen Rechtsunsicherheiten zu beseitigen.

Wir haben mit der Datenschutz-Grundverordnung eine große Chance, datenschutzfreundliche Rahmenbedingungen zu schaffen, auf die wir als Europäer stolz sein können.

Nutzen wir sie!