Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Vortrag

des Bundesbeauftragten für den Datenschutz
und die Informationsfreiheit

Prof. Ulrich Kelber

„Herausforderungen für den Datenschutz im Jahr 4 der DSGVO“

BvD Herbstkonferenz Datenschutz & Behördentag 2021

Berufsverband der Datenschutzbeauftragten
Deutschlands (BvD) e.V.

27.10.2021

Hybridveranstaltung

Es gilt das gesprochene Wort

Sehr geehrter Herr Spaeing, (Vorstandsvorsitzender des BvD e.V.),

liebe Kolleginnen und Kollegen, (Dr. Will und Dr. Brink),

sehr geehrte Damen und Herren,

ich danke für die Einladung.

Ich möchte den europäischen Blickwinkel ins Zentrum meiner Überlegungen stellen. Ähnlich wie der Urheber der Europahymne komme ja auch ich aus Bonn.

I. Einleitung

Ich erhoffe mir beim BvD natürlich ein Heimspiel. Schon in der Vergangenheit konnten wir auf Ihren Tagungen viele Gemeinsamkeiten feststellen, wenn es um den Schutz der Daten der Bürgerinnen und Bürger vor Übergriffen durch öffentliche, aber eben auch durch nicht-öffentliche Stellen geht.

Ich hoffe, es trübt unser Einvernehmen nicht, wenn ich Sie, lieber Herr Spaeing, beim Titel meines Beitrags ein wenig berichtige. Nicht aus Besserwisserei, sondern wegen einer wichtigen datenschutzpolitischen Botschaft:

Die DSGVO ist nicht in ihrem vierten Jahr. Sie ist bereits 2016 in Kraft getreten. Scharf gestellt wurde sie dann in der Tat zwei Jahre später. Insofern befinden wir uns heute bereits im sechsten Jahr der Datenschutz-Grundverordnung. Das Kind ist in der Schule angekommen, es wurde sogar schon evaluiert.

Und trotzdem funktioniert die Umsetzung der DSGVO noch immer an vielen Stellen nicht so, wie es sein sollte.

Meine Damen und Herren,

ich möchte aber den Blick nicht zurück, sondern in die Gegenwart und nach vorne richten. Das heißt: Wir müssen auch den Zusammenhang zwischen Versäumnissen bei der Umsetzung der DSGVO und dem technologischen Rückstand Europas gegenüber der Konkurrenz aus den USA und China unter die Lupe nehmen.

Die nationalen- und europäischen Datenschutz-Aufsichtsbehörden werden die große Aufgabe der Zukunft nicht allein bewältigen können. Hier kommt Ihnen, den betrieblichen Datenschutzbeauftragten, eine große Verantwortung zu. Sie wissen, wie ich Ihre Arbeit wertschätze.

II. Globale und technische Herausforderungen für den Datenschutz in Europa

Die nötige Umsetzung des europäischen Datenschutzrechts stellt hohe Anforderungen im Alltag von Betrieben, Behörden und Datenschutz-aufsichtsbehörden.

Wir würden uns die Bestandsaufnahme zu einfach machen, bliebe es bei der Betrachtung eher formaler rechtstechnischer Aspekte.

Wir müssen den Datenschutz auch vor dem Hintergrund weltweiter technologischer- und politischer Umwälzungsprozesse richtig einordnen und die notwendigen Konsequenzen ziehen.

Die Herausforderungen sind komplex und sie sind gewaltig. Erfolg ist keineswegs garantiert.

Ich nenne vier Stichworte:

- **Technologische Anforderungen an die DSGVO**
- **Der internationale Datentransfer**
- **Die DSGVO im ökonomische und politischen Härtetest mit den USA und China**
- **Der Erfolg der DSGVO: Nur durch Europa**

1. Technologische Anforderungen an die DSGVO

Als Informatiker und ehemaliger KI-Forscher könnte ich die vielfältigen Möglichkeiten dieser neuen Technik im Detail und mit viel Optimismus erläutern. Ich tue dies immer wieder gerne. Aber als Bundesbeauftragter für den Datenschutz ist es auch meine Aufgabe mit dafür zu sorgen, dass die KI nicht durch falsche Weichenstellungen zum Albtraum wird.

Mit Hilfe von Algorithmen und künstlicher Intelligenz können die großen Datensammelunternehmen, aber auch der Staat, ein sehr genaues Profil jedes einzelnen Menschen erstellen.

Ziel ist das maschinelle Lernen. Durch eine positive oder negative Rückkopplung soll das System zu einer „lernenden Maschine“ werden.

KI ist aus vielerlei Gründen fehlbar und intransparent, sie hat ihre Tücken und Fallstricke.

Zuallererst: Menschen machen Fehler während der Programmierung. Dass passiert beispielsweise im Design des Problems und des Optimierungsziels.

Es gibt auch noch weitere Fehlerquellen. So hängen die Ergebnisse eines KI-Systems ganz maßgeblich davon ab, wie es trainiert wurde. Wurde das System z.B. mit diskriminierenden oder zu selektiven Daten trainiert, kann sich dieser Prozess auch in den Entscheidungen dieses KI-Systems fortsetzen.

Wie alle anderen technischen Neuerungen darf auch die KI Menschen unter keinen Umständen zum Objekt machen. Deshalb müssen wir uns sehr genau überlegen, wo diese Verfahren eingesetzt werden dürfen, wo auf gar keinen Fall und wann welche Vorgaben gelten müssen. Die letzte Entscheidung bei allen wichtigen Fragestellungen muss immer einem Menschen vorbehalten werden. Selbstverständlich müssen auch zu jeder Zeit Korrekturen möglich sein.

Die Debatte über die europäischen Regelungen zur KI sind jetzt ein guter Zeitpunkt, diese Debatten zu führen und die richtigen Weichenstellungen vorzunehmen.

2. Der internationale Datentransfer

Datenübermittlungen sind grenzenlos. Der Datentransfer in andere Länder – oder zumindest in den Geltungsbereich ausländischen Rechts - gehört zu unserem Alltag wie der Stau auf der Datenautobahn.

Deshalb kann der Datenschutz nicht an den Grenzen enden.

Mit der DSGVO haben wir ein Regelwerk, das grundsätzlich weit über die europäischen Grenzen hinaus wirkt. Dafür sorgt beispielsweise das sog. **Marktordnungsprinzip.**

Wenn wir aber nicht den Datenschutz gegen den ökonomisch notwendigen gemeinsamen Datenraum der westlich orientierten Volkswirtschaften ausspielen lassen wollen, muss er **ein globales Anliegen** sein oder es noch werden. Gerade deshalb tauschen wir uns regelmäßig national und international mit Kolleg*innen aus.

Dass die DSGVO gut und wirksam ist, zeigen uns internationale **Entwicklungen wie die in Japan, Korea und Brasilien**, wo neue Datenschutzgesetze verabschiedet wurden. Deren Vorbild ist die DSGVO. Ebenfalls aus Japan kommt die Initiative FFoDwT, die wir mit offenen Armen aufnehmen und entwickelten sollten. Mit hohen Standards für den Datenschutz, das fordern unsere Grundwerte ein.

Die Rechtsprechung des EuGH und nicht zuletzt sein **Schrems II Urteil** vom 16. Juli 2020 ist im Hinblick auf den internationalen Datentransfer fundamental. Das Gericht hat auch dem letzten Zauderer unmiss-verständlich klargemacht, dass personenbezogene Daten von Bürgerinnen und Bürgern der EU nur dann an Drittländer weitergegeben werden dürfen, wenn sie dort einen im Wesentlichen gleichwertigen Schutz genießen wie in der EU.

Für die USA hatte der EUGH ein solches angemessenes Schutzniveau verneint. Was gilt dann wohl erst für China, Russland und die Türkei?

Ich erinnere noch einmal daran, dass der EuGH die Beurteilung einer datenschutzkonformen Übermittlung an Drittländer von den konkreten Umständen des Einzelfalls abhängig macht. Eine Musterlösung von der Stange kann und wird der Europäische Datenschutzausschuss daher auch in Zukunft nicht liefern. **Ich habe auf meiner Homepage ein Prüfungsschema veröffentlicht, wie mit dem Urteil umzugehen ist.**

Ich hoffe sehr auf ein internationales Übereinkommen zum grenzüberschreitenden Transfer personenbezogener Daten, dass mindestens zu Beginn die EU, Japan, Südkorea und Nord-Amerika umfassen sollten. Außerdem sollte es offen sein für Länder wie Indien, Mexiko, Australien, Brasilien etc.

Vielleicht haben wir endlich wieder die Chancen, ökonomische Interessen und Werte zusammenzuführen, auch in der Auseinandersetzung mit konkurrierenden Gesellschaftsentwürfen.

Auf **internationaler Ebene** findet ein breiter Austausch der Aufsichtsbehörden statt, wie zum Beispiel in der **Global Privacy Assembly (GPA**) letzte Woche. Darüber hinaus gibt es nun – dieses Jahr gestartet - auch einen Austausch innerhalb der **(neuen) G7-Gruppe**, wo ebenfalls eine intensive Diskussion zum internationalen Datentransfer stattfindet.

Die **Global Privacy Assembly** (GPA) ist die frühere Internationale Konferenz der Datenschutzbeauftragten, deren erstes Treffen 1979 in Bonn (Sie erinnern sich?) stattfand. Die GPA versteht sich als Ort des Erfahrungsaustausches und der gemeinsamen Befassung mit global relevanten Themen

Der **G7-Roundtable der Datenschutzbehörden** wurde von meiner britischen Kollegin Liz Denham im Kontext der diesjährigen G 7-Präsidentschaft des VK initiiert. Im Rahmen dieses Roundtable wurden engere Kooperationsmöglichkeiten zwischen den Datenschutzbehörden der G7 Staaten im digitalen Zeitalter eruiert und vereinbart. Dieses Jahr war das **Leitthema "Data Free Flow with Trust"** (DFFT). Nächstes Jahr liegt der Vorsitz bei mir.

Die G7-Behörden machten deutlich, dass technologische Entwicklungen und der immer bedeutendere internationale Datentransfer Hand in Hand mit der Einhaltung hoher Datenschutzstandards einhergehen müssen. Übergreifende Regulierungsansätze zwischen Datenschutz- und anderen Behörden, wie den Wettbewerbs- und Kartellbehörden, sind notwendig. Darüber hinaus brauchen wir eine Verständigung darüber, in welchem Ausmaß Zugriffe von Sicherheitsbehörden auf Daten in den globalen Kommunikationsnetzwerken aus dem Blickwinkel des Grundrechteschutzes tolerabel sind. Nur so gibt es Vertrauen.

Das Thema internationaler Datentransfer findet selbstverständlich auch auf nationaler Ebene statt. **Auch innerhalb der Datenschutzkonferenz und ihrer Arbeitsgruppen ist das Schrems II Urteil und damit auch der internationale Datenverkehr ein Dauerbrenner**.

Dazu wird der Kollege Brink bestimmt gleich etwas sagen.

Datenschutz ist weit mehr als ein in Recht gegossenes europäisches Grundrecht. **Datenschutz ist auch eine internationale Machtfrage.**

Die DSGVO hat viel bewegt. Die Begrenzung der Macht der dominierenden US-Technologie-Konzerne bleibt aber die bisher unbewältigte Herausforderung.

In der Pandemie ist die Macht dieser US-Riesen weiter gestiegen. Die DSGVO sollte eigentlich einen Werkzeugkasten für die Aufsichts-behörden liefern, um das datenschutzrechtliche Selbstbestimmungsrecht der Menschen – und damit auch unser Demokratieverständnis – vor dieser Macht zu schützen.

Ich kann hier nicht die DSGVO als großen Erfolg loben und zugleich über die Vollzugsdefizite bei ihrer Umsetzung den Mantel der barmherzigen Schweigsamkeit ziehen.

Es ist daher überaus misslich, dass sich Europa so schwer tut, wirksam gegen die die datenschutzrechtlich problematischen Verhaltensweisen der großen internationalen Datensammel-konzerne vorzugehen. **Das liegt auch daran, dass die feder-führenden Aufsichtsbehörden aus Irland und auch Luxemburg schlichtweg zu langsam agieren.**

Nach dem „**One-Stop-Shop-Verfahren“** ist bei grenzüberschreitenden Sachverhalten die Behörde am Sitz der Hauptniederlassung federführend zuständig. Irland ist von daher zuständig für viele Big-Tech-Unternehmen, da viele dieser Unternehmen aus steuerlichen Gründen ihren Hauptsitz für die EU in Irland haben. Hierzu gehören Microsoft, Apple, Facebook, Google sowie viele weitere.

Ich muss dies so offen ansprechen. *Wir sind ja unter uns*:

Irland ist „der Flaschenhals des Datenschutzes“.

Erfreulicherweise verhängten die Kollegen gegen **WhatsApp** ein saftiges Bußgeld in Höhe von 225 Millionen Euro. Das war allerdings eine überaus komplexe Zangengeburt. Am 28. Juli musste der **Europäische Datenschutzausschuss erst einen verbindlichen Streitbeilegungsbeschluss** nach Artikel 65 DSGVO fassen. Damit wurde die Streitigkeit über einen Beschlussentwurf der irischen Aufsichtsbehörde als federführende Aufsichtsbehörde für WhatsApp beendet, der wesentlich milder ausgefallen war.

Bei aller Freude über dieses erste große Verfahren gegen eine großen Player: Schaffen wir es nicht in näherer Zukunft, auch die Dutzenden grundsätzlichen weiteren anhängigen Verfahren gegen Facebook, Amazon und Co auf nationaler Ebene (Irland, Luxemburg) und sodann im Rahmen der EDSA-Beratungen abzuschließen, können wir Reputation und Akzeptanz des gesamten Regelwerks in die Tonne klopfen. Die Menschen verlören das Vertrauen.

Das ist nicht die Schuld der DSGVO. Sie schafft den geeigneten rechtlichen Rahmen. Der muss allerdings durch konkretes Handeln der zuständigen Aufsichtsbehörden durchgesetzt werden.

Hoffnungszeichen: Nach Kritik des EP haben nun das irische Parlament (mit klaren Worten) und auch die irische Regierung deutlich gemacht, dass man die DPC reformieren müsse.

Um den US-Datenkraken die überfälligen Grenzen setzen zu können, wird auch die Zusammenarbeit von Wettbewerbsschutz und Datenschutz immer wichtiger.

Was meine Behörde angeht, so arbeiten wir erfreulicherweise mit dem Bundeskartellamt immer öfter eng zusammen. Das Gleiche habe ich im EDSA, der GPA und der G7-Gruppe angeregt, zum Teil passiert es auch in anderen Ländern schon.

Meine Damen und Herren,

die Herausforderungen für Europa kommen aber beileibe nicht nur aus den USA.

Die womöglich noch schwerwiegenderen Probleme tun sich beim Umgang mit China auf.

Hier geht es nicht nur um wirtschaftliche Konkurrenz. Hier stehen sich auch diametral entgegengesetzte Werteordnungen gegenüber. Massenüberwachung, social score, Schutz von menschrenrechts-verletzenden Regimen, Hintertreiben von good governance in der Entwicklungszusammenarbeit.

Zur IT: Ich habe nicht die Sorge vor einem derartigen System des social credits in Deutschland oder ähnlicher Massenüberwachung in Europa. Demokratie und Rechtssaat sind stabil genug.

Angesichts immer neuer technischer Überwachungsmöglichkeiten darf uns aber dieser Befund nicht beruhigen. Die Digitalisierung ermöglicht auch hierzulande, unerschöpfliche Datenmengen aus den verschiedensten Lebens-bereichen zu verknüpfen und heimlich auszuwerten.

Das Gift staatlicher Totalkontrolle aus China und der privaten Überwachung durch US-Konzernen verpesten auch das Denken in Europa.

Hier ist die nächste Bundesregierung ebenso gefordert wie die anderen europäischen Regierungen, die Aufsichtsbehörden und die betrieblichen und behördlichen Datenschutzbeauftragten, den europäischen Weg nicht zu verlassen, China und USA nicht zu kopieren. Wirtschaftlicher Aufschwung kommt nicht dadurch, dass Europa China oder die USA kopiert.

4. Der Erfolg der DSGVO: Nur durch Europa

Deutschland verliert bei Innovations-Vergleich im internationalen Vergleich an Boden. Da mag der Eine oder die Andere denken, dass der Datenschutz doch eher froh sein kann, wenn er nicht ständig mit zu kurzen Beinen hinter der technischen Innovation herlaufen muss. Dieses Denken bringt uns aber nicht weiter: Im Gegenteil! Was nützen auch dem Datenschutz hiesige Produkte, wenn sie im internationalen Wettbewerb untergehen?

Nach dem jüngsten Global Innovation Index der der UN-Organisation für geistiges Eigentum fällt Deutschland im Ländervergleich bei Innovationen dramatisch zurück. Wir müssen sehr aufpassen. Sonst sind wir hier noch mehr auf Produkte aus China und den USA angewiesen.

Die DSGVO steht dem technischen Fortschritt und der Konkurrenzfähigkeit europäischer Waren und Dienstleistungen nicht im Weg: Ganz im Gegenteil. Sie ist ein Meilenstein, nicht nur für den Datenschutz. Sie stellt auch die Weichen für eine zukunftsweisende ökonomische Entwicklung, nämlich für europäische Produkte und Services, die auf den Weltmärkten vertrauenswürdig mit hoher Sicherheit und dem Schutz der Privatsphäre punkten. In Ländern, die den Datenschutz ebenfalls ernstnehmen und bei Bürger'innen, die um ihre Privatheit besorgt sind.

Zum ersten Mal haben wir in Europa ein einheitliches Datenschutzrecht mit vorbildlichen Schutzstandards. Auch **der Europäische Datenschutzausschuss EDSA kann mit Mehrheitsprinzip für die ganze EU verbindlich entscheiden.** Das täte übrigens auch innerhalb von Deutschland Not.

Bis Oktober 2021 hat der EDSA **40 Leitlinien zu zentralen Themen** angenommen oder bestätigt. Das betrifft Zertifizierungen und Akkreditierungen, den räumlichen Anwendungsbereich der DSGVO, Videoüberwachung, Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellung sowie das Recht auf Vergessen im Zusammenhang mit Suchmaschinen. Dazu gehören auch Fragen des prozessualen Ablaufs, beispielsweise bei Kooperations- oder Verfahren der Streitbeilegung.

An der Erarbeitung dieser Leitlinien haben sich die Datenschutzbehörden des Bundes und Länder in den zuständigen Expertenuntergruppen des Ausschusses intensiv beteiligt.

Neben den allgemeinen Leitlinien zur Auslegung der DSGVO hat der Ausschuss seit 2018 über 100 Stellungnahmen im Rahmen des Kohärenzverfahrens nach Art. 64 DSGVO zustande gebracht.

Diese Bilanz kann sich sehen lassen! Auch 1000 grenzüberschreitende Verfahren wurden eingeleitet, 200 davon abgeschlossen. Übrigens in keinem Land ist die Abschlussquote besser als in Deutschland.

Machen wir uns aber nichts vor. Der EU-Gesetzgeber hat nicht hinreichend bedacht, dass die von der DSGVO nicht harmonisierten nationalen Verfahrensordnungen bedenkliche Vollzugsdefizite produzieren können und auch produziert haben.

Die Effizienz des Vollzugs des EU-Rechs hängt nach wie vor maßgeblich von der Arbeit und der Entscheidungsfreude der federführenden nationalen Aufsichtsbehörde ab.

Mit ihrer Europäischen Datenstrategie und ihren jüngsten Gesetzesvorschlägen zur KI und zu den digitalen Märkten hat die Europäische Kommission ein weiteres Kapitel aufgeschlagen. Die nationalen Datenschutzaufsichtsbehörden und der EDSA müssen sich in diesem Diskussionsprozess das nötige Gehör verschaffen, das die Menschen in Europa von ihm erwarten.

Auch die ePrivacy-Verordnung ist überfällig, sie sollte eigentlich als bürgerrechtliches Pärchen mit der DSGVO 2016 in Kraft treten.

Kommission und Parlament waren mit gutem Beispiel vorangegangen. Was der Rat nun am 10. Februar 2021 beschlossen hat, ist ein Rückfall in die Zeit vor den Richtlinien von 1995.

Der Ratsentwurf macht Datenschutz zur Lachnummer, beispielsweise die nachträgliche Absegnung der berüchtigten „Cookie Walls“. So ganz nebenbei würden wichtige Garantien für Nutzerinnen und Nutzer gestrichen. Das Widerspruchsrecht oder die Datenschutz-Folgenabschätzung landeten in Ablage P wie Papierkorb. Sogar der Rückgriff auf die Garantien der DSGVO wurde aus dem Text verbannt. Bleibt es bei dieser Fassung der ePrivacy-Verordnung, könnten personenbezogene Daten ohne Einwilligung der Nutzenden auch relativ einfach zweckentfremdend weiterverarbeitet werden. Statt mehr Schutz für die besonders sensiblen Kommunikationsdaten atmet der gesamte Entwurf nur den Atem der kurzsichtigen Bedienung von Verwertungsinteressen bestimmter Datenhändler. Ausspionieren aber untergräbt eine freie Gesellschaft, egal ob durch den Staat oder durch Konzerne. Das sind leider keine guten Nachrichten aus Brüssel.

III. Schlussworte

Sie sehen, ich werbe für die DSGVO. Ich verschweige aber auch nicht deren Schwachstellen und Umsetzungsprobleme.

Die DSGVO kann - richtig verstanden und umgesetzt - die Menschen in den Stand versetzen, ihre digitale Zukunft selbst demokratisch mit zu gestalten und zu formen. Sie gilt eben auch für supranationale Konzerne.

Lassen Sie mich meinen Vorschlag wiederholen: Unser Ziel sollte es sein, weltweit Marktführer bei sicheren und datenschutzkonformen Produkten und Dienstleistungen zu werden. Datenschutzkonforme **Produkte „made in Europe**“ könnten sich als positives Differenzierungsmerkmal am Markt etablieren.

Warum nutzen wir in Europa nicht unseren Vorsprung mit .beim Datenschutz und bauen ihn zu einem Wettbewerbsvorteil aus? Mit unserem Datenschutzrecht und der Datenschutzgrundverordnung verfügen wir über einen glaubwürdigen Rechtsrahmen. Darum werden wir international beneidet, sie wird als Blaupause herangezogen.

Datenschutz und Datensicherheit sind unverzichtbare Erfolgsfaktoren und Qualitätsmerkmale im globalen Markt. Datenschutz muss daher von Anfang an als Teil der „DNA" eines jeden Produkts und einer jeden Dienstleistung mitgedacht werden.

Die Auseinandersetzung um das Verhältnis von Schutz personen-bezogener Daten und einer Lösung von Problemen wird uns weiter begleiten. Das geht nicht ohne Konflikte und Rückschläge und Diffamierungen des Datenschutzes in der Öffentlichkeit.

Was mich zuversichtlich stimmt: Umfragen mit offenen Fragestellungen ergeben breite Mehrheiten für mehr Datenschutz. Die öffentliche Meinung ist weiter als die veröffentlichte Meinung.

Ich möchte Sie bitten, ihre vielfältigen Einflussmöglichkeiten im Arbeitsalltag zu nutzen. Ich weiß, das ist oft konfliktträchtig. Aber machen Sie sich bewusst, dass Sie damit letztlich auch dem Unternehmen selbst dabei helfen, durch besseren Datenschutz und verstärkte Datensicherheit seine Wettbewerbsfähigkeit auch auf den internationalen Märkten zu steigern.

Lassen Sie sich nicht entmutigen.

Bleiben Sie hartnäckig und lassen Sie nicht locker.

Meine Mitarbeiter*innen und ich bleiben dabei zuverlässige Ansprech- und Kooperationspartner für Sie

Ich danke für Ihre Aufmerksamkeit