



**BfDI**

Der Bundesbeauftragte  
für den Datenschutz und  
die Informationsfreiheit

Vortrag

des Bundesbeauftragten für den Datenschutz

und die Informationsfreiheit

Prof. Ulrich Kelber

Euroforum Datenschutz

**Die DSGVO im Europäischen Datenschutzausschuss**

**- Beschlüsse, Ausblick -**

20 Minuten

05./06. 10. 2020

Es gilt das gesprochene Wort

Sehr geehrter Herr Prof. Wuermeling,

sehr geehrter Herr Prof. Forgo,

ich danke für die Einladung, heute über die DSGVO im Zusammenhang mit dem Europäischen Datenschutzausschuss zu sprechen.

Ihre Veranstaltung ist längst fester Bestandteil der Datenschutzdebatte in unserem Land.

Der heutige Vormittag steht ganz im Zeichen der Bilanz des neuen europäischen Rechts.

Ich freue mich auf den Gedankenaustausch: Es gibt viel zu bereden.

## I. Einleitung

Das mit gerade einmal 2,5 Jahren immer noch junge europäische Datenschutzrecht steht im Spannungsfeld vielfältiger, auch globaler Herausforderungen. Sie alle wirken unmittelbar auf die DSGVO ein.

Die Optimierung des Datenschutzrechts auf der Grundlage der von der EU-Kommission vorgenommenen Evaluierung ist eine wichtige Aufgabe. Das gilt gerade auch für die deutliche Verbesserung der Datenschutzaufsicht in der Praxis. Insofern steht die Evaluation mit ihren vielen Facetten zu Recht im Mittelpunkt dieser Tagung.

Wichtig ist es, bei der Debatte die **großen globalen Herausforderungen** nicht auszublenden.

Deshalb möchte ich – quasi als Türöffner für unsere Diskussion  
– die DSGVO in einen weiteren Zusammenhang stellen mit der

- politischen
- wirtschaftlichen
- und technologischen internationalen Entwicklung.

**Lassen Sie mich dieses Spannungsfeld darstellen:**

1. Der Aufstieg Chinas mit seinen globalen politischen, technologischen und ökonomischen Auswirkungen.
2. Die in der Corona-Krise weiter gewachsene Macht der US-Technologie-Konzerne in der Digitalen Revolution.
3. Die Covid-19-Krise mit ihren noch nicht absehbaren Herausforderungen und Langzeitwirkungen.
4. Die Revolution der technischen Entwicklungen.

## **II. Komplexe Herausforderungen für die DSGVO**

- **China und die Digitale Revolution der Unfreiheit**

In China herrscht eine immer autoritärere Partei mit allumfassender staatlicher Lenkung.

Der Staat macht klare Vorgaben. Trotzdem ist die Privatwirtschaft auf den Weltmärkten hoch präsent und nicht zuletzt im Bereich der Künstlichen Intelligenz äußerst wettbewerbsfähig.

KI ist in China nicht nur die neue Wunderwaffe für wirtschaftliche Expansion, sondern auch für die effektivere Ausgestaltung und Sicherung der autoritären Herrschaft.

**Das ist die Definition von Dual Use made in China.**

Chinesische Unternehmen können die ungehindert angefallenen riesigen Datenmengen als Turbo-Kraftstoff u.a. für die Weiterentwicklung der Künstlichen Intelligenz nutzen, die wiederum einen wesentlichen Beitrag dazu liefert, dass die allumfassende Nutzung dieser Daten omnipräsent wird.

China hat nicht zuletzt auch durch diesen totalitären Zugriff auf die Daten aller Bürgerinnen und Bürger vor allem im Vergleich zu europäischen Anbietern einen Vorsprung bei den KI-Technologien erreicht.

Besonders bedenklich in diesem Zusammenhang ist, dass die chinesische Regierung darüber hinaus noch europäische Unternehmen einlädt, in China Forschung und Entwicklung zu betreiben. Hierfür bietet man auch gerne mal den Zugriff auf eine Datenbank mit mehreren hunderttausenden Gesundheitsdaten der eigenen Bevölkerung an; Echtdaten selbstverständlich!

Es geht damit mittlerweile nicht mehr nur um die übliche Konkurrenz zwischen verschiedenen Anbietern auf den Weltmärkten.

**Es geht um die Konkurrenz unvereinbarer politischer, rechtlicher und ethischer Systeme.**

**Ein Wirtschaftswachstum auf Kosten von Grundrechten made in China kann und darf für uns in Europa niemals ein Vorbild sein!**

Und genau deswegen ist eine funktionierende DSGVO wichtig. Sie ist mehr als nur ein Regelwerk zur Verarbeitung von personenbezogenen Daten. Sie ist gleichzeitig die Verkörperung der freiheitlichen Idee von universell geltenden Grund- und Freiheitsrechten.

**Was folgt aus dieser Überlegung beispielsweise für die europäische Forschungspolitik?**

Sie muss nach meiner festen Überzeugung viel mehr als bislang datenschutzfreundliche Alternativen im Bereich der KI und anderer digitaler Innovationen fördern.

**Wir müssen mit dem Ehrgeiz an die Arbeit gehen, dass „Made in Europe“ auch auf den internationalen Märkten das erfolgreiche Gegenmodell zum autoritären chinesischen Weg und ein Benchmark für datenschutzfreundliche Produkte und Dienstleistungen wird.**

**Die Nachfrage dafür ist nicht nur in Europa groß**



- **Die wachsende Macht der US-Konzerne**

GAFAM waren schon vor der Corona-Krise die teuersten Unternehmen der Welt mit Finanzressourcen und Datenmassen, mit denen sie Einfluss ausüben und technologisch innovativere Konkurrenten verdrängen können. Und wenn nichts hilft, wird die Konkurrenz einfach aufgekauft.

Auch hier findet somit im Ergebnis eine Verschiebung der Technologiestandorte weg aus Europa statt.

Anders als in China werden die Menschen, deren Daten verarbeitet werden, hier zwar nicht unterdrückt. Einen gleichwertigen Schutz ihrer Persönlichkeitsrechte wie hier in Europa gibt es aber grundsätzlich auch nicht.

Auch deshalb ist die DSGVO wichtig. Mit ihrem Marktortprinzip setzt sie auch für die großen US-Konzerne Grenzen und ermöglicht eine Kontrolle zum Schutz der europäischen Bürgerinnen und Bürger.

**Bessere Kontrolle allein wird aber nicht ausreichen.**

**Europa muss sich vielmehr auch als Antwort auf die die  
aktuelle Krise technologisch endlich emanzipieren.**

Der Markt ist da. Die Nachfrage nach datenschutzfreundlicher IT ist so groß wie nie zuvor. Der europäische Markt hat hier eine Gelegenheit, mit eigenen Angeboten ein Benchmark und damit auch die Konkurrenz unter Zugzwang zu setzen.

Leider wird in der deutschen Wirtschaft beim Thema Datenschutz immer noch zu viel gejammert und zu wenig unternehmerisch gehandelt!

Währenddessen reiten amerikanische Unternehmen wie Apple immer mehr auf der „Privacy-Welle“ und investieren seit einigen Jahren hohe Millionenbeträge in Werbung, die gerade die datenschutzfreundlichen Features ihrer Produkte hervorhebt.

Der ehemalige Gouverneur von Virginia, Terry McAuliffe, hat vor kurzem in einer Kolumne gewarnt, dass die USA Gefahr laufen könnten, ihre politische und ökonomische Vorreiterrolle zu verlieren, wenn man nicht ein nationales Datenschutzrecht etablieren würde.

Hier sehen wir die Ausstrahlwirkung, die die DSGVO bis in die USA hinein hat. Momentan sieht es danach aus, dass die USA es besser schaffen, diese für sich nutzbar zu machen als deutsche und europäische Unternehmen, die immerhin auf eine jahrzehntelange Expertise im Bereich des Datenschutzes zurückblicken können.

**Diese Erfahrungen zu nutzen und auf Basis der DSGVO eine weltweite Vorreiterrolle bei datenschutzfreundlichen Angeboten einnehmen - das sollte Anspruch der deutschen Wirtschaft sein.**

Wer nur auf die Wirtschaft zeigt, macht es sich allerdings auch zu einfach. Auch die Datenschutzaufsichtsbehörden müssen ihren Teil leisten, um das mit der DSGVO erstrebte Level-Playing-Field tatsächlich zu erreichen.

Als Erstes müssen die europäischen Aufsichtsbehörden das in der DSGVO geregelte Verfahren der Zusammenarbeit im Europäischen Datenschutzausschuss besser nutzen. Da ist noch ziemlich viel Luft nach oben.

**Datenschutzverstöße müssen zeitnah und so effektiv wie möglich von der zuständigen federführenden Behörde geahndet werden, einschließlich der Verhängung von Bußgeldern.**

Nur so besteht die Chance, globale Technologie-Konzerne auf die Einhaltung der europäischen Spielregeln zu verpflichten und Raum für europäische Konkurrenten zu schaffen.

Auch nach 2,5 Jahren Scharfstellen der DSGVO gibt es noch immer in keinem der wichtigen Verfahren Entscheidungen gegen die großen US-Datenverarbeiter. Das ist völlig inakzeptabel.

- **Die Corona-Krise und der Datenschutz**

Die Herausforderungen für den Datenschutz sind durch die Pandemie noch größer, noch dringlicher geworden.

**Corona ist in vielen Bereichen, auch bei der Digitalisierung und dem Datenschutz, zu einem Prozessbeschleuniger geworden.**

Auch das Ritual der Klagen aus der Wirtschaft über zu viel Bürokratie als Hindernis für den Wirtschaftsaufschwung nach der Krise gehört zur politischen Folklore.

Bei aller im Einzelfall nachvollziehbaren Kritik an der einen oder anderen Schwachstelle der DSGVO:

**Die Wirtschaft sollte beim Datenschutz kein Roll Back  
anpeilen.**

Punkten sollte sie lieber mit datenschutzfreundlichen Lösungen.  
Das wäre auch gut für die Bilanzen.

**Meine Damen und Herren,**

**Datenschutz und moderne Informationstechnologie:**

**Das gehört zusammen.**

**Wir sehen das am Beispiel der sog. „Corona-Warn-App“**

Hier wurde ein datenschutzfreundliches Produkt unter  
Beteiligung der Datenschutzaufsichtsbehörde von Beginn  
entwickelt.

Die App wurde in Deutschland fast 19 Millionen Mal  
heruntergeladen. Häufiger als in allen anderen europäischen  
Staaten zusammen

Die Warn-App ist – bei aller Unkerei und aller berechtigter Kritik im Detail - längst zu einem nationalen und internationalen Erfolg geworden. Mittlerweile bedienen sich mehrere Länder an dem Open-Source-Code des deutschen Projektes.

**Ein Grund für diesen Erfolg ist das Vertrauen in das Produkt und seinen zuverlässigen Datenschutz.**

Möglich macht das die DSGVO. Sie ermöglicht nämlich eine rechtmäßige Verarbeitung von sensiblen Gesundheitsdaten.

**Damit steht der Datenschutz weder der Forschung im Speziellen noch der Pandemiebekämpfung im Allgemeinen entgegen.**

Sowohl in der Forschung als auch bei der Nachverfolgung von Kontakten sind datenschutzfreundliche und transparente Lösungen erfolgreich.

**Aber trotz dieser Erfolge können wir uns nicht nur freuen.**

**Es bleibt bei der technischen Abhängigkeit der Warn-App von den Smartphone-Systemen von Apple und Google.**

Daran ändert auch nichts die nach Aussagen der Entwickler gute Zusammenarbeit mit diesen US-Unternehmen

Die versichern zwar, dass sie die Daten ausschließlich zweckgebunden und datenschutzkonform verarbeiten.

**Hier müssen die Aufsichtsbehörden genau hinzuschauen.**

Bei einem Verstoß käme das maximale Bußgeld nach der Datenschutzgrundverordnung in Betracht. Bei Apple sprechen wir da über mehr als 10 Mrd. US-Dollar.

Diese scharfen Sanktionsmöglichkeiten wiederum verdanken wir der DSGVO.



- **Die technische Revolution**

Alle 10 Jahre steigt die Leistungsfähigkeit der Speichergeräte um den Faktor 25. Schon diese eine Zahl macht die ganze Tragweite der Veränderungen deutlich.

Ganze Berufszweige und Branchen und Geschäftsmodelle werden sich durch die Digitalisierung radikal verändern oder ganz verschwinden.

Diese technische Entwicklung ist unaufhaltsam.

Auf die anstehenden Veränderungen muss sich die Gesellschaft aber vorbereiten. Sie muss – anders als in China, in einem demokratischen und rechtsstaatlichen Rahmen stattfinden.

Das heißt, Ängste zu nehmen und die sozialen Folgen der Digitalisierung abmildern.

Das heißt, Chancen für alle eröffnen, in dem man diese Veränderung mit Umsicht gestaltet und Rahmenbedingungen setzt, auch rechtlicher Art.

Eines ist dabei klar: Die Bereitschaft, diesen Wandel mitzumachen, sich für Digitalisierung zu öffnen, hängt – wie die Corona Warn App beweist – vor allem mit Vertrauen zusammen. Vertrauen in Ihre Produkte und Dienstleistungen. Vertrauen in die Durchsetzung von Spielregeln auch in der digitalisierten Welt.

### **III. Der Evaluierungsbericht der EU-Kommission**

Die Evaluierung der DSGVO wird noch in einigen weiteren Beiträgen detailliert behandelt, daher will ich sie an dieser Stelle nur kurz anreißen.

Zunächst bin ich froh über die positive Gesamtbewertung der DSGVO im Evaluationsbericht der EU-Kommission vom 24. Juni 2020.

Dieser belegt aber auch, wo es noch klemmt. Und das ist gut so! Der Kommission und auch den Aufsichtsbehörden ist durchaus klar, dass die **DSGVO in bestimmten Bereichen eine Herausforderung ist.**

Gerade kleinere, aber auch mittlere Unternehmen erleben die DSGVO teilweise als eine schwierige Operation. Davon können alle Aufsichtsbehörden ein Lied mit vielen Strophen singen.

Auf Grund des risikobasierten Ansatzes lassen sich aber nun einmal allein auf die Größe von Unternehmen bezogen keine Ausnahmen von der DSGVO stützen. Die Großbäckerei ist datenschutzrechtlich eben nicht sensibler als die deutsche Niederlassung von Tik-Tok.

Das macht es für Startups, Handwerker, kleine  
Gewerbetreibende und Vereine ganz gewiss nicht leichter.

Ich teile deshalb nachdrücklich das Verlangen der Kommission  
an die Aufsichtsbehörden, für diese Unternehmensgruppen  
weitere Hilfestellungen anzubieten. **Helfen geht vor Strafen.**

**Dann müssen aber auch alle Aufsichtsbehörden genug  
Ressourcen für Beratung haben.**

### **Nationale Datenschutzaufsicht**

Weiterentwicklungsbedarf sehe ich bei der nationalen  
Datenschutzaufsicht.

Seit einiger Zeit liegt ein Antrag des niedersächsischen  
Wirtschaftsministeriums auf dem Tisch, der die Verlagerung der  
Datenschutzaufsicht für den gesamten nichtöffentlichen Bereich  
auf die Bundesebene fordert. Beklagt wird vor allem die

fehlende Einheitlichkeit und Verbindlichkeit der Entscheidungen der deutschen Aufsichtsbehörden.

Auch die Kartellrechtskommission 4.0 hat sich für Veränderungen der Datenschutzaufsicht ausgesprochen.

Das gilt auch für die Datenethikkommission, deren Mitglied ich war. Ihr geht es dabei allerdings primär um die Verstärkung und Formalisierung der Abstimmung zwischen den Behörden.

Die DSK ist kein offizielles Gremium mit eigener Exekutivbefugnis. Ihr fehlt eine gesetzliche Grundlage.

Man könnte aber zumindest ohne großen Aufwand durch ein ständiges Sekretariat der DSK eine optimale Vorbereitung auch dann möglich ermöglichen, wenn kleine Datenschutzbehörden den Vorsitz der Konferenz oder der Arbeitsgruppen haben.

Wir 18 Datenschutzbehörden sollten uns außerdem in der Aufsichtspraxis einheitlich an die Beschlüsse, Leitlinien, Orientierungshilfen der DSK halten; auch wenn wir einmal selbst überstimmt wurden.

**Und wir müssen in der DSK schneller werden beim Finden gemeinsamer Standpunkte.**

Innerhalb der Datenschutzkonferenz haben wir mit einer Arbeitsgruppe „Datenschutzkonferenz 2.0“ auf diese Herausforderung reagiert.

### **Verbesserung der europäischen Datenschutzaufsicht**

Anders als bei der DSK hat die Datenschutzaufsicht in der EU mit dem Europäischen Datenschutzausschuss (EDSA) ein Gremium, in dem wir verbindliche, EU-weit gültige Beschlüsse fassen könnten.

In vielen eigentlich dringenden Fällen konnten wir dies aber noch nicht, weil vor allem die federführenden irischen und luxemburgischen Aufsichtsbehörden bis heute keinen Beschlussvorschlag vorgelegt haben. Das betrifft fast alle Beschwerden zu Facebook, Google, Amazon und Microsoft.

**Das macht den EDSA aktuell faktisch zu einer „lame duck“.**

**Das Schrems-II-Urteil und die 101 Beschwerden von NYOB sind nun Risiko und Chance für den EDSA zugleich.**

Die eingereichten 101 Beschwerden wenden sich nicht gegen Google und Facebook selbst, sondern gegen Firmen, die Google Analytics und Facebook Connect integrations nutzen.

In Deutschland betreffen die Beschwerden übrigens acht Unternehmen.

Dadurch können bzw. müssen sich nun die Aufsichtsbehörden der einzelnen Mitgliedstaaten eigenständig der Beschwerden annehmen, ohne auf eine Grundsatzentscheidung aus Irland angewiesen zu sein.

Da den Beschwerden von Bürgerinnen und Bürgern aber grundsätzlich ein gemeinsames Problem zu Grunde liegt, muss es letztendlich auch eine einheitliche gesamteuropäische Linie bei der Lösung dieses Problems geben.

Die Ergebnisse der Prüfung in Spanien dürfen am Ende nicht von denen in Deutschland oder Schweden abweichen.

**Sonst ginge Vertrauen in das gemeinsame europäische Recht verloren.**

Daher ist es richtig und wichtig, dass sie die Mitglieder des EDSA hier eng abstimmen. Gelingt es in diesen Fällen die Funktionsfähigkeit der DSGVO und des Kohärenzmechanismus zu bestätigen, wäre dies ein Meilenstein für eine dauerhaft bessere Zusammenarbeit im EDSA.



**Gelingt es hingegen nicht, wäre dies im schlimmsten Fall der Anfang vom Ende des EDSA in seiner jetzigen Form.**

Um letzteres – losgelöst von den aktuellen NOYB-Beschwerden – zu verhindern, bin ich fest davon überzeugt, dass wir einen **grundlegenden Reformbedarf beim One-Stop-Shop** haben.

Wichtige Fälle sollten künftig direkt dem EDSA zugeteilt werden. Der bräuchte dafür eine Arbeitsebene, auf der diese Fälle auf Basis eines europäischen Verfahrensrechts zügig geklärt werden können.

#### **IV. Offene Punkte im Europäischen Datenschutzrecht**

Ich möchte abschließend noch ein paar kurze Bemerkungen zu einigen Themen machen, die für die Weiterentwicklung des Europäischen Datenschutzrechts wichtig sind.

Ich hätte gerne im Kommissionsbericht ein paar Aussagen gehört zu einigen wichtigen Fragen wie dem Thema **Scoring und Profiling**.

Moderne Datenverarbeitung ermöglicht das Anlegen, die Auswertung und Analyse ungeheurer Datenmengen aus verschiedensten Kontexten.

Selbstlernende Algorithmen eröffnen immer neue Möglichkeiten, das Verhalten von Menschen vorherzusagen und sogar zu steuern. Das geht längst über Kreditentscheidungen und Anzeigenschaltung hinaus.

Wir brauchen eine europäische Verschärfung des geltenden Rechtsrahmens, um die Menschen vor Manipulation und Diskriminierung wirkungsvoll zu schützen.

Meine Haltung wird von der Konferenz der Datenschutzbeauftragten ebenso geteilt wie von der **Datenethikkommission**.

Die vorhandenen **Regelungen der DSGVO** sollten sich **bereits auf die Bildung von Profilen erstrecken und nicht nur** auf die automatisierte Entscheidungsfindung, die in der Praxis umgangen wird. Beim Erlaubnisvorbehalt und den Betroffenenrechten.

**Die Datenethikkommission will** verschiedene Formen der algorithmenbasierten Entscheidung – und damit unter anderem auch des Profilings – **anhand ihres Risikopotentials klassifizieren und regulieren.**

Das richtet sich etwa nach dem Einsatzzweck und der Sensibilität der Daten.

Ich halte diesen Vorschlag für sehr vernünftig.

In jedem Fall muss der europäische Gesetzgeber bei der ungehemmten Nutzung personenbezogener Daten zur Profilbildung auf die Bremse treten.

**Er muss dringend effektive Grenzen setzen.**

Und ich möchte auf Ergebnisse nicht bis zum nächsten Evaluierungsbericht im Mai 2024 warten müssen.

## **Verbraucherschutz stärken**

Ich habe eingangs angemerkt, dass der Erfolg der DSGVO als Bürgerrecht in der Europäischen Demokratie vom Vertrauen der Menschen in ihre Wirksamkeit abhängt.

Hier stimmt mich eine aktuelle Untersuchung zuversichtlich und nachdenklich zugleich.

Die von OpenText in Auftrag gegebene Umfrage wurde von April bis Mai 2020 über Google Surveys unter 12.000 Verbrauchern aus Deutschland, dem Vereinigtem Königreich, Frankreich, Spanien, Kanada, Australien und Singapur durchgeführt.

**Zuversichtlich** stimmt mich, dass Datenschutz danach den deutschen Verbraucherinnen und Verbrauchern viel wert ist. Viele sind sogar bereit, mehr Geld bei Unternehmen auszugeben, die persönliche Daten ihrer Kunden schützen.

**Besorgt** bin ich, weil fast die Hälfte der Befragten den deutschen Unternehmen nicht zutraut, die Daten sicher und vertraulich zu behandeln. Unsicherheit und Misstrauen sind bei 47 Prozent vorhanden.

Im weltweiten Vergleich steht Deutschland in Sachen Misstrauen auf dem ersten Platz – dicht gefolgt vom Vereinigten Königreich (45 %) und Kanada (40 %).

Nur sechs Prozent der deutschen Befragten vertrauen Unternehmen in ihren Datenschutz-Kompetenzen – das ist deutlich zu wenig.

#### **IV. Schlussbemerkung**

Die DSGVO wird als großes europäisches Projekt bestehen bleiben

Statt immer neuer Einwürfe und Forderungen nach Aufweichung bewährter Schutzstandards, wie im aktuellen Papier deutscher Wirtschaftsverbände, sollte ein in die Zukunft gerichteter Dialog erfolgen. Dieser muss die grundlegenden Werteentscheidungen des neuen europäischen Datenschutzrechts respektieren und seine Umsetzung weiterentwickeln.

**Ich danke Ihnen für Ihre Aufmerksamkeit.**