Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Vortrag

des Bundesbeauftragten für den Datenschutz
und die Informationsfreiheit

Prof. Ulrich Kelber

„Das BayLDA der Gegenwart – Föderaler Datenschutz im europäischen Verbund“

beim Symposium

„20 Jahre Datenschutz in Mittelfranken - mehr als ein Jahrzehnt Landesamt für Datenschutzaufsicht“

des Bayerischen Landesamtes für Datenschutzaufsicht - BayLDA

Ansbach, 23. Juni 2022

Es gilt das gesprochene Wort

Sehr geehrte Damen und Herren,

lieber Michael Will,

I. Einleitung

Zunächst möchte ich mich für die Einladung zu der heutigen Veranstaltung bedanken.

Ich wäre heute aus zwei Gründen gerne bei Ihnen in Ansbach gewesen: Weil ich gebürtiger Franke bin und vor allem, weil ich die Arbeit, die das BayLDA für den Datenschutz im nicht-öffentlichen Bereich leistet, außerordentlich schätze.

Das BayLDA hat nach meinem Eindruck seit seiner Gründung immer großen Wert darauf gelegt, die Persönlichkeitsrechte der Bürgerinnen und Bürger zu schützen und zugleich den bayerischen Unternehmen mit einem guten Blick für das praktisch Umsetzbare als Ratgeber bei der Umsetzung der nicht immer einfachen datenschutzrechtlichen Anforderungen zur Seite zu stehen. Und wenn es darauf ankommt, scheut das BayLDA auch nicht die klare Anordnung, die Verhängung einer Geldbuße und die gerichtliche Auseinandersetzung. Ich freue mich insbesondere auch deshalb, heute bei Ihnen zu sein und gratuliere herzlich zum Jubiläum.

II. Entwicklung in den vergangenen 20 Jahren

Blicken wir auf die Gründung der Bayerischen Datenschutzbehörde für den nicht-öffentlichen Bereich unter dem Dach der Regierung von Mittelfranken vor 20 Jahren zurück, wird sehr deutlich, dass sich in der Zwischenzeit auch aus Sicht der deutschen Aufsichtsbehörden viel verändert und getan hat.

Zum einen wurden insbesondere wir deutschen Aufsichtsbehörden dahingehend gestärkt, unsere Aufgaben in völliger Unabhängigkeit wahrzunehmen. Unabhängige Aufsichtsbehörden sind ein wichtiger Faktor, um das Unionsrecht durchzusetzen und im Bereich des Datenschutzes eine einheitliche Rechtsanwendung zu schaffen.

So wurde knapp zehn Jahre nach der angesprochenen Gründung auch das BayLDA als unabhängige Behörde, damals noch mit dem hoch angesehenen Herrn Kranig als Präsidenten an der Spitze, errichtet.

Zum anderen waren die letzten zwanzig Jahre natürlich auch von der zunehmenden Digitalisierung - gerade auch im Privatbereich - geprägt. Immer mehr digitale Produkte und Dienstleistungen wurden insbesondere auch für Verbraucher und Verbraucherinnen entwickelt und zu erschwinglichen Preisen auf den Markt gebracht.

Vor zwei Jahrzehnten war die E-Mail das wahrscheinlich am meisten verbreitete elektronische Kommunikationsformat; sie wurde aber kaum von den meist teuren mobilen Endgeräten abgeschickt, sondern oft noch von großen Desktoprechnern. Die mobile Textkommunikation beschränkte sich auf SMS – auf 160 Zeilen begrenzt, teuer und über die Nummerntasten des Mobiltelefons eingetippt. An Smartphones oder Tablets war noch nicht wirklich zu denken.

In den vergangenen zehn Jahren wurde diese Art der Kommunikation insbesondere auch durch die mögliche mobile Nutzung von Messengerdiensten wie WhatsApp, Threema oder Signal auf hochmodernen Smartphones ergänzt und mitunter sogar fast vollständig abgelöst.

Auch durch die in Deutschland ab Mitte der Nuller Jahre zunächst durch soziale Netzwerke und später dann durch Plattformen wie „Instagram“ oder „YouTube“ ermöglichte Erstellung von privaten Profilen bzw. der Einstellung privater Videos, die u.a. den kompletten Tagesablauf der Nutzerinnen und Nutzer zum Zweck der Selbstdarstellung für eine ungefilterte Öffentlichkeit preisgeben, hat sich die Nutzung des Internets durch Privatpersonen nachhaltig gewandelt:

Diente sie vor zwei Jahrzehnten noch vornehmlich der Information des Menschen durch Inanspruchnahme der angebotenen Medien, so fließen die Daten zwischenzeitlich nicht mehr vornehmlich von den Medien aus zu den Menschen, sondern, wie die angeführten Beispiele zeigen, auch von den Menschen in alle möglichen Richtungen.

Zudem werden immer mehr Alltagsgegenstände mit Sensoren ausgestattet und vernetzt. Daher ist neben dem gerade angesprochenen „herkömmlichen“ Internet auch das „Internet der Dinge“ ein zentraler Treiber für das Datenwachstum.

Als Reaktion auf diese Entwicklung werden wir gegenwärtig unter anderem von Seiten der Europäischen Kommission geradezu von einem Feuerwerk von Gesetzgebung überzogen. Mit dem so genannten Digitalpaket der EU soll eine neue Architektur aus besserem Datenzugang und stärkerer Kommerzialisierung von Daten entstehen.

Zuletzt sei in diesem Kontext auf den pandemiebedingten Schub der Digitalisierung in den letzten zwei Jahren hingewiesen, durch den neben dem privaten inzwischen auch der berufliche Lebensbereich stark durchdrungen wird.

Personenbezogene Daten haben folglich gerade in der digitalisierten Welt eine herausragende Bedeutung: Denn sie fallen hier besonders viel und umfangreich an und sind schnell und einfach zugänglich. Wir Menschen produzieren so viele Daten wie nie zuvor. Wir alle hinterlassen tagtäglich und fortwährend Datenspuren, eigentlich eher dichte Datenwolken in der digitalen Welt.

Und diese Daten werden von einigen Akteuren zu umfassenden Persönlichkeitsprofilen verarbeitet. Und das keineswegs nur, um gezielter Anzeigen zu verbreiten.

Ob wir ein Spiel nutzen, uns auf einer Website über eine Krankheit informieren oder einfach nur unterwegs sind und das Handy in der Tasche haben. Überall werden wir beobachtet und ausspioniert. Das ist das Krebsgeschwür der Digitalisierung, das hält eine freie Gesellschaft nicht aus, dem muss konsequent ein Riegel vorgeschoben werden, auch wenn manche Lobby dann protestiert.

III. Digitalisierung als Herausforderung auch für die DSK

Die personenbezogenen Daten fallen unter den Schutz der DSGVO. Daher galt und gilt es auch aus datenschutzrechtlicher Sicht, mit dieser zunehmenden Digitalisierung Schritt zu halten.

Die DSK setzt sich seit jeher dafür ein, dass jeder Mensch tatsächlich selbst entscheiden können muss, welche Daten und Datenspuren er hinterlässt und wie diese verwertet werden.

1. In der Vergangenheit

Blicken wir 20 Jahre zurück, wird deutlich, dass sich die DSK schon immer den mit dem Datenwachstum aufgrund der technologischen Entwicklung verbundenen Herausforderungen angenommen hat.

So wird beispielsweise bereits in der Entschließung der 63. DSK (7./ 8. März 2002 in Mainz) zum „Umgang mit personenbezogenen Daten bei Anbietern von Tele-, Medien- und Telekommunikationsdiensten“ bekräftigt, dass durch den Anstieg der Internetnutzung dem

datenschutzgerechten Umgang mit den dabei anfallenden Daten immer größere Bedeutung zukommt.

Weiter hat die DSK darin quasi als Vorreiter eine anlasslose und massenhafte Speicherung von Verkehrsdaten durch die gerade genannten Anbieter abgelehnt und dadurch das Recht auf informationelle Selbstbestimmung betroffener Personen gestärkt. Das Ergebnis der DSK wurde Jahre später durch die bekannte Entscheidung des BVerfG aus 2010 zur Vorratsdatenspeicherung gestützt. Auch der EuGH hat mit seinen Entscheidungen in 2014 und zuletzt im April diesen Jahres der anlasslosen und unbegrenzten Vorratsdatenspeicherung eine grundsätzlich Absage erteilt.

In der Entschließung der 65. DSK (27./28. März 2003) „Forderungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder an Bundesgesetzgeber und Bundesregierung“ sensibilisiert die DSK für die Problematik von zunehmender Registrierung und Überwachung, die durch immer umfassendere Datenverarbeitungsbefugnisse, zunehmenden Datenhunger sowie immer weitergehende technische Möglichkeiten zur Beobachtung und Durchleuchtung der Bürgerinnen und Bürger entstehen. Als Lösungsansätze wurden bereits damals u.a. **die Förderung von datenschutzgerechter Technik und die Gewährleistung einer anonymen Internetnutzung** genannt.

2. und aktuell

Wie die beiden von mir herausgepickten Beispiele zeigen, haben wir deutschen Aufsichtsbehörden bei unserer Arbeit selbstverständlich auch immer die aktuellen Entwicklungen in Folge der zunehmenden Digitalisierung im Auge. So möchten wir uns in der DSK im Hinblick auf die entsprechende Forderung aus dem aktuellen Koalitionsvertrag auf Bundesebene in Kürze u.a. auch damit befassen, wie eine **anonyme und pseudonyme Online-Nutzung** nachhaltig gewährleistet werden kann.

Durch die fortschreitende Digitalisierung und den verstärkten Einsatz von KI enthalten die gewonnenen Informationen größere Aussagekraft und sind damit neben der wirtschaftlichen Verwertung auch in Feldern wie der **wissenschaftlichen Forschung** von immer größerem Interesse.

Hier werden personenbezogene Daten in vielen Bereichen verarbeitet. Während diese Verarbeitung in Forschungsfeldern wie der Psychologie oder der Humanmedizin unerlässlich und bekannt ist, da der Mensch hier im Zentrum der Forschung steht, findet in anderen Forschungsfeldern wie der Umwelt- oder Geowissenschaften eine weniger offensichtliche Verarbeitung personenbezogener Daten statt.

Die Nutzung personenbezogener Daten ist für eine gute wissenschaftliche Forschung essentiell. Sie bietet enormes Potenzial, das zum Wohle des Einzelnen und der Allgemeinheit genutzt werden kann. Das geltende Datenschutzrecht erkennt dieses Potenzial vor dem Hintergrund des erklärten Ziels der EU, den wissenschaftlichen Fortschritt zu fördern und dauerhaft einen europäischen Forschungsraum zu schaffen, durch eine Reihe weitreichender Privilegierungen prinzipiell an.

Um eine wissenschaftliche Forschung, die sich nach unseren europäischen Werten richtet, zu fördern und die in der DSGVO enthaltenen Öffnungsklauseln für den Bereich der Forschung auch rechtlich auszufüllen, haben wir deutschen Aufsichtsbehörden zu dieser Thematik auf der 103. DSK eine Entschließung verabschiedet und darin folgendes festgehalten:

„Die DSGVO zielt daher darauf ab, einen Ausgleich zwischen der Forschungsfreiheit auf der einen Seite und dem Recht des Einzelnen auf Achtung seines Grundrechts auf Datenschutz zu schaffen. So weist Artikel 89 DSGVO darauf hin, dass Verarbeitungen von personenbezogenen Daten für die wissenschaftliche Forschung geeigneten Garantien für die Rechte und Freiheiten der betroffenen Personen im Sinne der DSGVO unterliegen, mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet werden muss. Die DSK unterstützt daher nachdrücklich die Förderung und Erforschung von Methoden, Forschungsdaten so zu verarbeiten, dass Persönlichkeitsrechte der Bürgerinnen und Bürger bestmöglich geschützt werden. Soweit ein Zugriff auf identifizierende Angaben nicht durch

geeignete innovative Methoden ausgeschlossen werden kann, sollten Anonymisierung, Pseudonymisierung, Datentreuhänderschaften und andere Instrumente vorgesehen werden.“

Durch diese Entschließung haben wir zum Ausdruck gebracht, dass wissenschaftliche Forschung und Datenschutz gerade auch aus Sicht der DSK miteinander vereinbar sind. Uns war jedoch auch wichtig klar zu machen, dass der Datenschutz auch hier von Anfang an mitgedacht werden muss und Instrumente genutzt werden müssen, die dem Schutz der persönlichen Daten dienen. Neben der Rechtsklarheit für die Nutzung von Forschungsdaten muss daher der Schutz für die personenbezogenen Daten der Bürgerinnen und Bürger sichergestellt werden. Eine Scheuklappen-Digitalisierung, die nur das Ziel einer Datenverarbeitung in den Blick nimmt und auf dem Weg dorthin nicht Datensicherheit und Datenschutz so ausgestaltet, dass die Grund- und Freiheitsrechte der Bürgerinnen und Bürger optimal geschützt werden, die lehnen wir vehement ab.

Aus diesem Grund begrüßt die DSK ausdrücklich das im Koalitionsvertrag der Bundesregierung formulierte Vorhaben, ein Forschungsdatengesetz zu schaffen, das die Persönlichkeitsrechte wahrt. Flankiert werden sollte dieses allgemeine Forschungsdatengesetz durch Forschungsregelungen in einzelnen Bereichen, wie es beispielsweise für den Bereich der Gesundheitsdaten bereits in Planung ist.

Abschließend zu diesem Thema erlaube ich mir auch an dieser Stelle einen kurzen Schwenk auf die Arbeit der DSK in den vergangenen 20 Jahren, in dem ich Ihnen mitteile, dass die DSK bereits seit über 15 Jahren ein Forschungsdatengesetz fordert, auch um mehr Forschung mit personenbezogenen Daten zu ermöglichen. Traurig, dass der Gesetzgeber da bisher untätig geblieben ist.

IV. EDSA/Internationales

Von Bayern und Franken in die Welt: Es ist ein oft gehörter Allgemeinplatz, dass die Datenverarbeitung global stattfindet und daher auch die Datenschutzaufsicht zu globalen Standards und einer länderübergreifenden Zusammenarbeit und Durchsetzung des Datenschutzes kommen muss. Dieser Befund gilt auch für Deutschland und erst Recht gilt er für die Landesaufsichtsbehörden in unserem föderalen Aufsichtssystem.

So macht eben auch die Datenverarbeitung bayerischer Unternehmen nicht an bayerischen Grenzen halt. Nicht zuletzt deshalb ist das BayLDA heute ein wichtiger, kompetenter und hoch anerkannter Player im europäischen und internationalen Konzert.

- In den vergangenen 20 Jahren, hat sich das BayLDA im EDSA und seinen Subgroups vor allem einen Namen im wichtigen Bereich der international Transfers und der entsprechen ITS Expert Subgroup gemacht. Hier besteht eine langjährige Expertise beim LDA, die sich auch im AK der DSK niederschlägt.

Im Drittstaatentransfer hat sich in den letzten Jahren viel getan. Denken wir alleine an die Konsequenzen aus dem Schrems II-Urteil. Ein wichtiger Schritt im Hinblick auf die Umsetzung der Ergebnisse des Schrems II-Urteils war die Arbeit der vom EDSA eingesetzten Taskforce Supplementary Measures

- Im Juni 2021 nahm der EDSA Empfehlungen zu den „zusätzlichen Maßnahmen“ in ihrer endgültigen Fassung nach öffentlicher Konsultation an. Die Empfehlungen sollen Datenexporteure bei der Bewertung unterstützen, ob bei einer Übermittlung von Daten an Drittländer zusätzliche Maßnahmen erforderlich sind. Die Empfehlungen enthalten dazu praktische Beispiele für verschiedene Übermittlungsszenarien. Außerdem findet sich in einem Annex eine nicht abschließende Liste möglicher zusätzlicher Maßnahmen, wie z. B. einer Datenverschlüsselung.

- Dieses wichtige Papier hat Auswirkungen an vielen Stellen, unter anderem beim sog. Coordinated Enforcement Framework. Der CEF ist zusammen mit der Einrichtung eines Expertenpools (Support Pool of Experts, SPE) eine Schlüsselmaßnahme des Europäischen Datenschutzausschusses (EDSB). Die beiden Initiativen zielen darauf ab, die Durchsetzung und die Zusammenarbeit zwischen den Aufsichtsbehörden und eine gleichförmige Umsetzung des Rechts zu verbessern. Die erste koordinierte Durchsetzungsmaßnahme des Europäischen Datenschutzausschuss umfasst 22 Aufsichtsbehörden, die Untersuchungen über die Nutzung von Cloud-basierten Diensten durch den öffentlichen Sektor eingeleitet haben.

- Damit sind wir im Bereich der Compliance und der Durchsetzung der DSGVO. Die DSGVO bietet ein umfangreiches und sehr wirksames Instrumentarium für die Einhaltung einer Compliance durch den Verantwortlichen an. Art. 5 der DSGVO listet die Grundsätze der Verarbeitung personenbezogener Daten auf. Prinzipien wie „privacy by design“, „privacy by default“ oder die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung für die Verarbeitungen mit hohem Risiko, z.B. beim Einsatz neuer Technologien, setzen z.B. weitere Eckpunkte.

- Weiter sind die Aufsichtsbehörden im Sinne eines Enforcement mit einem umfangreichen Katalog an Befugnissen ausgestattet, von der einfachen Warnung über Anweisungen bis hin zu Geldbußen. Und diese Geldbußen sind mit den bekannten Schwellen von 2% oder sogar 4% gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres eines Verantwortlichen empfindlich und werden auch ernst genommen. So wie auch im Wettbewerbsrecht, aus dem diese Konstruktion entlehnt ist.

- Die Zusammenarbeit der nationalen Behörden auf Ebene des EDSA muss auch noch verbessert werden, gerade in den Big-Tech-Fällen. Es ist kein Geheimnis, dass der OSS-Mechanismus noch nicht „effektiv“ greift. Erläuterung OSS. Hier können wir als Aufsichtsbehörden sicher noch effektiver werden, um nachhaltig den Datenschutz zu stärken.

- Im EDSA haben wir erkannt, dass wir für ein effektives Enforcement den OSS-Mechanismus weiter stärken müssen und uns im April auf konkrete Schritte hierzu verständigt. Um die in der DSGVO vorgesehenen Möglichkeiten der Zusammenarbeit so effizient wie möglich zu nutzen, werden wir jährlich eine Reihe von grenzüberschreitenden Fällen von strategischer Bedeutung ermitteln, für die ein Aktionsplan mit einem festen Zeitplan für die Zusammenarbeit festgelegt wird. Alle Mitglieder des EDSA sind zu einer engen Zusammenarbeit verpflichtet, und wir konzentrieren uns auf praktische Lösungen, um die Kapazitäten der Datenschutzbehörden in der Durchsetzung zu stärken.

- Gruppen von Datenschutzbehörden können beschließen, ihre Kräfte bei Ermittlungs- und Durchsetzungsmaßnahmen zu bündeln, und Datenschutzbehörden können die Arbeit innerhalb dieser Gruppen teilen. Bei Bedarf kann eine EDSA-Taskforce eingesetzt werden.

Darüber hinaus verpflichten sich die Datenschutzbehörden, Informationen über nationale Durchsetzungsstrategien auszutauschen, um auf Ebene des EDSA jährliche Durchsetzungsprioritäten zu vereinbaren, die sich in den nationalen Durchsetzungsprogrammen widerspiegeln können. Die Datenschutzbehörden können einen gemeinsamen Durchsetzungsrahmen einschließlich gemeinsamer Instrumente für Kontrollen ausarbeiten.

V. Schlussbemerkung

Bei all durch unsere Aufgabe als Datenschutzbehörden verursachten Vorbehalten gegen bestimmte Vorgehensweisen in der Digitalisierung ist es mir wichtig, zum Abschluss noch einmal zu betonen, dass die sich hieraus ergebenden Veränderungen vor allem enorme Chancen für jeden Einzelnen, für unsere Gesellschaft und für unser Miteinander mit sich bringen.

Nehmen Sie neben dem eingangs aufgeführten Bereich der Forschung, die völlig neuen Teilhabemöglichkeiten, die beispielsweise daraus resultieren, dass geballtes Wissen, nun – quasi auf Knopfdruck – für jedermann zur Verfügung steht.

Wir müssen die **Chancen der Digitalisierung** nutzen. An dieser Stelle möchte ich wie so oft jedoch daran erinnern, dass wir hierbei auch und gerade um einen Freiraum zur unbeobachteten persönlichen Entfaltung zu belassen, immer auch die **Privatsphäre schützen** müssen:

Digitalisierung, die den Menschen im Blick hat, muss immer auch die Anforderungen des Datenschutzes berücksichtigen. Um Vertrauen und Sicherheit zu schaffen und zugleich wirtschaftlich und verantwortlich zu handeln, ist es unerlässlich, den **Schutz personenbezogener Daten und die Freiheit und das Selbstbestimmungsrecht des Einzelnen** bei der Entwicklung von Produkten und Dienstleistungen –ebenso wie ich es gerade schon für den Bereich der Forschung aufgeführt habe- von Anfang an mitzudenken und entsprechend zu berücksichtigen.

Auch für uns Aufsichtsbehörden gilt es, ein waches Auge für die Risiken und Nebenwirkungen, aber auch für die Chancen der Digitalisierung zu haben. Entscheidende Faktoren sind hier verstärkte Sensibilisierung und Aufklärung.

Dabei wollen wir uns nicht nur als Mahner hervortun und damit riskieren, Wasser auf die Mühlen derjenigen geben, die Datenschutz als Hemmschuh und Bremsklotz der digitalen Innovation darstellen. Vielmehr wollen wir mit nach Lösungen für eine datenschutzfreundliche Digitalisierung suchen und die Vorteile, die diese mitbringen, aktiv betonen. Denn ich denke, dass mir niemand hier widersprechen wird, wenn ich sage, dass z.B. eine gutgemachte und abgesicherte digitale Lösung aus datenschutzrechtlicher Sicht immer besser ist als eine ausufernde analoge Zettelsammlung.

Für einen Ausblick, was (darüber hinaus) auf die Datenschutzaufsicht zukommt, bin ich auf die Diskussion im nachfolgenden Programmteil gespannt.

Ich danke Ihnen für Ihre Aufmerksamkeit.