Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Vortrag

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Prof. Ulrich Kelber

Kedua Datenschutztag 2020

Das Erfolgsmodell DSGVO wird evaluiert – - Wie geht es weiter in Europa?

Video für den 09.06.2020

9.35 Uhr bis 10.15 Uhr vorgesehene **Redezeit**

I. Einleitung

Sehr geehrte Damen und Herren,

liebe Datenschützerinnen und Datenschützer,

Gerne hätte ich heute auch direkt mit Ihnen gesprochen. Wir alle haben uns aber ja in den letzten Monaten an die digitale Kommunikation gewöhnt. Und so hoffe ich doch, dass Sie meine Gedanken auch auf diesem Weg erreichen.

Mein Thema war – schon lange vor Corona –

„Das Erfolgsmodell DSGVO wird evaluiert – wie geht es weiter in Europa?“

Niemand von uns konnte bei der Planung dieser Veranstaltung ahnen, dass sich der Fokus der gesamten politischen und gesellschaftlichen Diskussion so verschieben würde, wie wir das seit dem Frühjahr erleben.

Auch im Datenschutz erleben wir durchaus ein Vorher und ein Nachher.

II) Die DSGVO in der Corona-Krise

Die Pandemie hat die **„Bewährungsauflagen“** für den Datenschutz sogar noch erhöht. Die DSGVO steht selbst zwei Jahre nach ihrem „Scharfstellen“ nach Meinung vieler Beobachter und Akteure noch immer unter „Bewährung“.

Die Herausforderungen sind möglicherweise sogar noch größer, noch dringlicher geworden.

Dabei müssen wir aufpassen, dass die DSGVO nicht in eine Art Kreuzfeuer gerät.

Für die einen steht sie wegen zu viel Bürokratie dem wirtschaftlichen Aufschwung im Wege - andere wiederum beklagen, der Datenschutz sei - wie andere Grundrechte auch - „unter die Räder“ eines Notstandsregimes geraten.

1. Datenschutz vs. Wirtschaft?

Der Datenschutz muss sich daher gerade in der aktuellen Situation der politischen Debatte mit beiden Gegenpositionen auseinandersetzen.

Was die Vorwürfe aus der Wirtschaft angeht, ist diese Debatte nicht neu. Sie begleitet die DSGVO seit ihrer Entwicklung. Sie ist auch meist frei von empirisch belegbaren Fakten.

Von den unterschiedlichen Interessengruppen werden aktuell ihre alte Forderungen (weniger Datenschutz, Abbau von Klimaschutz, neue Steuervorteile etc.) hervorgekramt.

Auch sonst unverkäufliche Ladenhüter werden plötzlich zum vermeintlichen Wundermittel des Wirtschaftswachstums.

So mehren sich bereits Stimmen, die sich das „Hochfahren“ der Wirtschaft nicht ohne eine gründliche Entsorgung von Datenschutzvorschriften vorstellen können. So zuletzt der BDI.

Das Gleiche gilt für Klimaschutz, Diversität, Mindestlohn und eine wertegeleitete Außenpolitik.

Zukunftsgewandt und nachhaltig sind solche Forderungen nicht: Ganz im Gegenteil.

Ich sehe in der Krise sogar eine Chance für die Wirtschaft, endlich mit datenschutzfreundlichen Lösungen zu punkten. Nehmen wir beispielsweise den Technologie-Sektor: Homeoffice, Videokonferenzen und gemeinsames digitales Arbeiten wurden stärker denn je zuvor zu einer Notwendigkeit für viele von uns. Dabei werden viele Arbeitgeber, die diesen Themen bislang eher skeptisch entgegen standen festgestellt haben, dass diese neue Art des Arbeitens sehr gut funktionieren kann.

Ich rechne daher damit, dass wir auch nach der Krise ein weiterhin großes Interesse an entsprechenden Produkten und damit einen Markt haben werden, an dem Anbieter ein echtes Gewicht in die Waagschale werfen könnten, wenn ihre Lösungen im Sinne von privacy by design und privacy by default datenschutzfreundlich ausgestaltet wären.

Denn dass Daten- und Grundrechtsschutz den Menschen wichtig ist, können wir ebenfalls als eindeutige Erkenntnis aus dieser Krise mitnehmen. Die Debatte um die Corona-Tracing-App ist hier nur eines von vielen Beispielen.

Der Markt hat zu wenig im Angebot, die Nachfrage ist riesengroß. Es kommt mir ein wenig wie beim Ökolandbau und der Elektromobilität vor: Der Markt in Deutschland (und Europa) wächst, aber das Angebot aus Deutschland kommt nicht hinterher, so dass Anbieter von außerhalb das Rennen machen.

2. Der wirksame Schutz der Bürgerrechte durch die DSGVO Debatte

Lassen Sie mich meine Position über die Schutzwirkung der DSGVO an vier Punkten erläutern:

1. **Die Bedeutung der Grundrechte im Notstandsfall**
2. **Die DSGVO als datenschutzrechtliche Leitlinie**
3. **Die DSGVO als gesamteuropäisches Gesetzeswerk mit weltweiter Ausstrahlung**
4. **Die Weiterentwicklung der DSGVO (Evaluierung)**

Zu 1. Die Bedeutung der Grundrechte im Notstandsfall

Die Klage über das Ende der Grundrechte ist nicht mehr nur im Internet weit verbreitet.

Sie findet auch auf der Straße statt.

Machen wir uns nichts vor: Die Eingriffe in die Religions- und Versammlungsfreiheit sowie in die Berufsfreiheit und einer Reihe anderer Grundrechte sind in der Geschichte der Bundesrepublik ohne Beispiel. Das kann man feststellen, ohne deswegen gleich zum Aluhutträger, Reichsbürger oder ähnlichem mutieren zu müssen.

Aber ich stimme dem gerade aus dem Amt geschiedenen Präsidenten des Bundesverfassungsgerichts, Herrn Voßkuhle, aus Überzeugung zu, dass die Grundrechtsordnung der Bundesrepublik Deutschland nicht in Gefahr ist; auch weil die Rechtsprechung in den vergangenen Wochen klargestellt hat, dass die Anforderungen an deren Beschränkungen sehr hoch sind. Das bestärkt meine Zuversicht.

Trotzdem ist höchste Wachsamkeit - auch der Datenschutzaufsicht - dringend geboten:

Administrative Beeinträchtigungen sind in jedem Fall zeitlich streng zu begrenzen. Sie müssen auch in jedem Fall sorgfältig begründet werden. Und sie benötigen klare rechtliche Grundlagen.

Allgemeine Aussagen wie „Der Schutz des Lebens geht immer vor“ oder „Gesundheitsschutz vor Datenschutz“ reichen dafür nicht aus.

In jedem Einzelfall gelten:

- die Grundsätze des Gesetzesvorbehalts
- und der Verhältnismäßigkeit
- sowie der parlamentarischen Kontrolle.

Es gibt keinen Grund, nach dem Motto „Not kennt kein Gebot“ rechtsstaatliche Schutzmechanismen über Bord zu werfen. Gerade in der Not bewährt sich der Rechtsstaat.

Auch unter hohem Zeitdruck lassen sich beispielsweise auf der Grundlage der DSGVO und des BDSG freiheitliche und datensparsame Lösungen entwickeln. Dies gilt für den Lockdown selbst ebenso wie für die Datenverarbeitungen, die als Voraussetzungen für seine Aufhebung betrachtet werden.

Ich verweise hier auf das Papier der DSK vom 13. April.

Datensparsame Konzepte blockieren und hemmen nicht.

Sie tragen vielmehr zur besseren Effektivität und Effizienz des jeweiligen Datenverarbeitungssystems bei. Denken Sie nur an die datenschutzwidrigen und auch völlig ungeeigneten Ideen aus Ende März, mit Mobilfunkzellendaten Kontaktpersonen zu ermitteln. Heute sind alle froh, dass wir Datenschützer das schon im Keim erstickt haben, es hätte schlicht nicht funktioniert. Damals wurden wir regelrecht beschimpft, uns sei die Gesundheit der Bevölkerung wohl völlig egal.

Angesichts der öffentlichen Verwirrung durch die wachsende lokale Aufsplitterung der Schutzmaßnahmen werden die Menschen nur digitalen Systemen vertrauen, die sie nicht ausspähen und in deren Folge keinerlei Repressalien zu erwarten sind.

Zu 2. **Die DSGVO als datenschutzrechtliche Leitlinie**

Transparenz der Maßnahmen zur Bekämpfung der Pandemie ist eine zwingend notwendige Voraussetzung für die Unterstützung der Bevölkerung.

Lassen Sie mich an dieser Stelle ein paar Anmerkungen zur sog. **„Corona-Warn-App“** machen:

Gerade aufgrund der scharfen Einschränkung von Grundrechten hat die Einschätzung von unabhängigen Aufsichtsbehörden ein großes Gewicht, wenn es um die Akzeptanz der App in der Gesellschaft geht.

Dementsprechend sind sie auch rechtzeitig und umfänglich bei grundrechtserheblichen Maßnahmen zur Pandemiebekämpfung einzubinden, damit sie ihrer Beratungsaufgabe nachkommen können.

Und das geschieht auch meistens!

Vom Prinzip der Transparenz und der Datenminimierung gesehen ist der dezentrale Ansatz datenschutzfreundlich. Ich freue mich, dass sich diese Position durchgesetzt hat.

Es bleibt natürlich dabei, dass die Warn-App technisch von den Smartphone-Systemen von Apple und Google abhängig ist.

Diese versichern, die Daten ausschließlich zweckgebunden und datenschutzkonform zu verarbeiten.

Hier müssen die Aufsichtsbehörden genau hinzuschauen. Bei einem Verstoß käme das maximale Bußgeld nach Datenschutzgrundverordnung in Betracht. Also vier Prozent des weltweiten Jahresumsatzes des jeweiligen Konzerns. Bei Apple waren dies zuletzt 260 Milliarden US-Dollar.

Diese scharfen Sanktionsmöglichkeiten verdanken wir der DSGVO. Das neue europäische Datenschutzrecht bietet eine Möglichkeit, bestimmte Folgen dieses ökonomischen Machtgefälles wenigstens abzumildern.

Dennoch bleibt die Achillesferse des europäischen Datenschutzes bestehen, die chronische Abhängigkeit der Digitalisierung in Europa von den führenden US-Konzernen.

Über die Entwicklung der App hinaus werden diese als Monopolanbieter gerade auch in der Folge der Krise noch mächtiger. Amazon verdrängt zunehmend den lokalen Einzelhandel und auch der digitale Schub durch Bestellsysteme und Videokonferenzen etc. nützt überwiegend den US-Marktführern. Gerade deshalb verlangt die aktuelle Krise einmal mehr, sich technologisch zu emanzipieren. Aus wirtschaftlichen Gründen, aber auch aus Sicht des Datenschutzes, um nicht in die Situation des „Vogel friß oder stirb“ zu bleiben bzw. zu geraten.

Apple, Google, Facebook, Microsoft und Amazon waren schon vor der Krise die teuersten Unternehmen der Welt.

Gerade die US-Konzerne verfügen jetzt über noch mehr Finanzressourcen und Datenmassen, mit denen sie Einfluss ausüben und Konkurrenten verdrängen können. Deswegen wird übrigens auch die Zusammenarbeit von Wettbewerbsschutz und Datenschutz immer wichtiger werden.

Die Macht dieser Unternehmen beschränkt sich längst nicht mehr – wie vielfach angenommen – auf direkte wirtschaftliche Belange wie personenbezogene Werbung etc.

Wer über die persönlichen Daten verfügt, übernimmt auch mit die Lenkung und Kontrolle ganzer Branchen und darüber hinaus der Gesellschaft.

Betroffen ist daher nicht allein der Rechtsstatus einzelner betroffener Personen. Betroffen ist die Demokratie in ihrer Gesamtheit.

Ich will mit aller Klarheit deutlich machen: Bekommt Europa mit seinem Datenschutzrecht die Datenriesen und ihre Geschäftsmodelle nicht in den Griff, ist die DSGVO gescheitert.

Wir müssen hier eine digitale Souveränität entwickeln.

Daher müssen künftig alle europäischen Aufsichtsbehörden das in der DSGVO geregelte Verfahren der Zusammenarbeit im Europäischen Datenschutzausschuss besser nutzen und das Verfahren auch bei den großen, grundsätzlichen und grenzüberschreitenden Verfahren mit Leben füllen.

Deshalb ist es von zentraler Bedeutung, dass die Datenschutzbehörden der EU-Mitgliedsstaaten die Möglichkeiten der DSGVO tatsächlich nutzen.

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 von Spielregeln zu verpflichten.

Nur durch solch entschlossenes Handeln könnten wir die Konzerne wirksam und nachhaltig im Interesse der Menschen bewegen, die Vorschriften der DSGVO einzuhalten.

Das nach zwei Jahren noch in keinem der wichtigen Verfahren eine Entscheidung auch nur ansteht, ist inakzeptabel.

Zu 3. Die DSGVO als gesamteuropäisches Gesetzeswerk

Erst die DSGVO hat wirklich zu einem einheitlichen europäischen Vorgehen im Datenschutz geführt.

1.Der EDSA als Kern des europäischen Datenschutzes

Der Europäische Datenschutzausschuss (EDSA) hat am 21. April zwei neue Leitlinien zum Datenschutz während der Pandemiebekämpfung veröffentlicht. Mit seinen Beschlüssen gibt der EDSA Hinweise zum Umgang mit Gesundheitsdaten für Forschungszwecke und zu Grundsätzen von Tracking Tools. Beide Leitlinien nehmen direkten Bezug auf den Ausbruch von COVID-19.

Ich bin froh darüber, dass wir uns auf europäischer Ebene auf das Bekenntnis zur Freiwilligkeit verständigt haben. Sowohl in der Forschung als auch bei der Nachverfolgung von Kontakten können nur solche Lösungen erfolgreich sein, die transparent sind und ohne Zwang funktionieren.

Es muss eindeutig und leicht verständlich sein, zu welchem Zweck die Daten erhoben und wann sie wieder gelöscht werden.

Ein individuelles Tracking oder eine spätere Re-Personalisierung müssen ausgeschlossen sein.

Diese Grundsätze werden wir als Aufsichtsbehörde von Verantwortlichen und Entwicklern in allen 27 MS-Staaten und auch den Staaten des EWR einfordern.

Der EDSA hat in seiner Stellungnahme darauf aufmerksam gemacht, dass die DSGVO sehr forschungsfreundlich gestaltet ist.

Der Datenschutz steht weder der Forschung, noch der Pandemiebekämpfung entgegen.

Die DSGVO ermöglicht eine rechtmäßige Verarbeitung von sensiblen Gesundheitsdaten. Gleiches gilt für den Einsatz von digitalen Hilfsmitteln zur Pandemiebekämpfung.

Klar ist aber auch, dass Apps und andere Werkzeuge kein Ersatz sein können für ein funktionierendes Gesundheitssystem und gegenseitige Rücksichtnahme.

Und klar ist, dass das Grundrecht auf Privatsphäre und informationelle Selbstbestimmung nicht eingeschränkt werden darf und auch nicht eingeschränkt werden muss, um die Pandemie zu bekämpfen.

2. Der Fall Ungarn: Eine Bewährungsprobe für die europäischen Bürgerrechte

Wie wichtig das einheitliche europäische Recht zum Schutz der Bürgerinnen und Bürger gerade in Krisenzeiten ist, zeigt das Verhalten der Regierung Orban.

Sie hat durch Dekret weitreichende Einschränkungen der Betroffenenrechte verordnet. Private und öffentliche Verantwortliche dürfen Betroffenenrechte pauschal bis zum Ende des Corona-Notstands mal so eben aussetzen.
Die Anträge betroffener Personen sollen erst am Tag nach dem Ende des Notstands bearbeitet werden. Ohne zeitliches Limit.
Ob der vorgesehene 20. Juni für das Ende der Maßnahmen eingehalten wird, muss sich zeigen.

Beschränkungen der Betroffenenrechte sind nach Art. 23 DSGVO jedoch nur unter engen Voraussetzungen möglich. Wie ausgefeilt das in der DSGVO geregelt ist, zeigt sich daran, dass die Bekämpfung einer Pandemie grundsätzlich als "Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses ... im Bereich der öffentlichen Gesundheit" zulässig sein kann. Das regelt Art. 23 Abs. 1 lit. e DSGVO.

Ich habe aber massive Zweifel, ob in Ungarn die Verhältnismäßigkeit gegeben und der Wesensgehalt der Grundrechte und Grundfreiheiten gegeben sind. Ich bezweifle sowohl die Geeignetheit, die Erforderlichkeit, als auch deren Verhältnismäßigkeit im engeren Sinne angeht.
Es kommen nämlich wie die Erfahrungen hierzulande zeigen, weitaus mildere Mittel in Betracht.

Viele Betroffenenrechte lassen sich nun einmal nicht wie der Konsum von Kartoffelchips auf einen späteren Zeitpunkt verschieben. Werden unrichtige Daten nicht berichtigt (Art. 16 DSGVO), kann ein irreversibler Schaden entstehen.

Das Dekret von Herrn Orban erfindet zu allem Übel auch noch eine zusätzliche Frist für die Ausübung der Rechtsbehelfe nach Art. 77 - 79 DSGVO. Das ist ein massiver Verstoß gegen die DSGVO.

Für die Ausübung des Beschwerderechts bei einer Aufsichtsbehörde und den gerichtlichen Rechtsschutz gibt es keinerlei Beschränkungsmöglichkeiten in der DSGVO.

Nicht nur ich selbst, auch andere Mitglieder des EDSA, bezweifeln die Wirksamkeit der ungarischen Notstandsdekrete zur Bekämpfung der Corona-Pandemie. Zeitlich unbefristete Sonderkompetenzen der Regierung sind hier wegen Verstoßes gegen höherrangiges Recht unwirksam bzw. unanwendbar.

Ich frage mich, was Europa ohne die wirksamen Instrumente der DSGVO tun könnte, um die Rechte der Menschen in Ungarn vor den Übergriffen ihrer eigenen Regierung zu schützen?

Die alte Richtlinie hätte dies so nicht leisten können.

Zu 4. Die Weiterentwicklung der DSGVO (Evaluierung)

1. Trotz holprigem Start ein Erfolg

Bei aller Freude über Vorzüge und Erfolge der DSGVO auch in der Pandemie-Krise, möchte ich doch ihren holprigen Start in Erinnerung rufen. Wir erinnern uns: Das Internet war voll mit gezielt verbreiteter Verängstigung, aber auch glatten Fehlinformationen.

Eine Abmahnwelle wurde heraufbeschworen – ein Tsunami an Kostenbescheiden und Bußgeldern gegen kleine Unternehmen und Vereine zog am dunklen Horizont herauf. Manche schwafeln heute noch davon. Faktenfrei – Spaß dabei

Manche Unsicherheiten konnten durch die Aufklärungsarbeit der Aufsichtsbehörden gerade gerückt werden. Mit einer besseren Vorabinformation wären vielleicht viele dieser Horrorszenarien nicht auf einen so fruchtbaren Boden gefallen. Hier hätten die Wirtschaftsverbände, die Regierung und – bei rechtzeitiger personeller Aufstockung - auch die Aufsichtsbehörden bessere Arbeit leisten können.

Ich hätte mir gewünscht, dass die Medien nicht jeden Quatsch ungeprüft verbreitet hätten, sondern sich auf den wichtigen journalistischen Grundsatz der Recherche besinnen würden.

Diese Besorgnisse und Ängste waren unbegründet. Trotzdem sind Angst- und Miesmacherei noch längst nicht beendet. Sie werden jetzt in der aktuellen Krise mal wieder hervorgekramt.

Ich möchte Sie ermutigen, sich nicht mit der bloßen Zurückweisung dieser Anwürfe zu begnügen.

In der Diskussion haben wir allen Grund, gemeinsam und offensiv die Fortschritte durch die DSGVO in der öffentlichen Debatte hervorzuheben:

- Mit der DSGVO haben die Betroffenen mehr Kontrolle und Transparenz bei der Datenverarbeitung erlangt.
- Die Europäische Union hat endlich Schluss gemacht mit dem nationalstaatlichen und extrem löchrigen Flickenteppich beim Datenschutz.
- Das Datenschutzbewusstsein ist in dieser Zeit merklich gestiegen. Die Eingaben bei den Aufsichtsbehörden haben sich vervielfacht.
- **Die DSGVO ist ein internationales Erfolgsmodell**. Über 100 Ländern dieser Welt haben inzwischen Datenschutzgesetzes eingeführt. In der Mehrzahl außerhalb von Europa – gerade in Afrika. Vielerorts wurde – z. B. in Kalifornien und in Brasilien – die DSGVO als Vorbild herangezogen.

2. Evaluierung als gesamteuropäischer Lernprozess

Die DSK hat ihren Bericht über die Erfahrungen auf der 98. Konferenz verabschiedet und dem EDSA zugeleitet. Der wurde von der Kommission nach Art. 97 Abs. 3 DSGVO konsultiert.

Gut, dass wir uns in dem doch recht aufwändigen Verfahren auf eine anspruchsvolle Reformagenda verständigen konnten.

Gut auch, dass wir uns auf wesentliche Punkte konzentriert und nicht die alten Schlachten bei der Entwicklung der DSGVO nochmal geschlagen haben.

Lassen Sie mich einige Reformbaustellen im laufenden Evaluierungsprozess herausgreifen, die mir besonders am Herzen liegen und die wir auch in der aktuellen Krisenlage nicht aus den Augen verlieren dürfen:

1.1 Das 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.

Die Verarbeitung ihrer Daten kann Betroffenen nützen, aber auch erheblich schaden.

Ich nenne hier als Stichwort für Gefahren die chinesische Überwachungsstrategie gegenüber der eigenen Bevölkerung; aber auch die Vermessung der Bürger durch US-amerikanische Privatfirmen.

Die **DSGVO** enthält zwar eine Definition des Profilings in Art. 4 Nr. 4 und das Verbot reiner automatisierter Entscheidungsfindung in Art. 22. Sie bleibt aber letztlich **vage und lückenhaft**. Rechtlich auf dem Stand von 1995. Technisch auf dem Stand der 1980er Jahre.

Wir müssen an dieser Stelle – wenn irgend möglich auf europäischer Ebene - nachbessern. Nationale Alleingänge sind der falsche Weg.

Wir brauchen eine **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, in der ich mitgearbeitet habe.**

Die vorhandenen **Regelungen der DSGVO** sollten sich **bereits auf die Bildung von Profilen erstrecken und nicht nur** auf die automatisierte Entscheidungsfindung.

Die Auskunfteien mit der Schufa vorweg beteuern stets, dass sie ja selbst gar keine automatisierten Entscheidungen treffen. Sie stellten dem Endkunden lediglich Profil und Score zur Verfügung.

Auch bei den Banken verfehlen häufig die Schutzregelungen bei der automatisierten Entscheidungsfindung ihr Ziel: Sie berufen sich treuherzig auf eine menschliche Entscheidungsinstanz. Die ist zumindest auf dem Papier vor einer Kreditvergabe dazwischen geschaltet.

Deshalb sollte bereits das Profiling als solches dem Verbot mit Erlaubnisvorbehalt des Art. 22 DSGVO unterstellt wird.

Zudem müssen die Betroffenen generell ein Recht auf aussagekräftige Informationen haben, wenn Profilbildung stattfindet.

Große Sympathie habe ich auch für einen in diesem Zusammenhang relevanten Ansatz der Datenethikkommission.

Danach sollen verschiedene Formen der algorithmenbasierten Entscheidung – und damit unter anderem auch des Profilings – **anhand ihres Risikopotentials klassifiziert und reguliert werden**.

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

Ergibt sich ein unvertretbares Risikopotential, kann es ggf. zum vollständigen Verbot kommen.

In jedem Fall steht der europäische Gesetzgeber vor der Aufgabe, der ungehemmten Nutzung personenbezogener Daten zur Profilbildung effektive Grenzen zu setzen.

1.2. Maßvolle Entbürokratisierung statt Kahlschlag bei den Bürgerrechten

Die Kolleginnen und Kollegen aus den Ländern und auch mich erreichen immer wieder Beschwerden über den bürokratischen Aufwand durch die DSGVO.

Ich sehe durchaus Bereiche, in denen sich der bürokratische Aufwand reduzieren lässt, ohne gleichzeitig den Datenschutz zu beschneiden.

Ich denke an die Informationspflichten, die gerade für kleine Unternehmen und Vereine einen maßgeblichen Mehraufwand im Vergleich zum alten Datenschutzrecht mit sich bringen.

Ich wehre mich aber gegen jeden Kahlschlag:

Die **Informationspflichten** der Art. 13 und 14 DSGVO sind ein **Kernstück der DSGVO**.

Transparenz ist zum einen die Voraussetzung für die Ausübung der Betroffenenrechte. Zum anderen ist das Wissen darüber, wer welche meiner Daten zu welchen Zwecken verarbeitet aber auch ein Wert für sich.

In einer **digitalen Umgebung** sind **diese Informationspflichten regelmäßig gut erfüllbar**.

Die Informationen können grundsätzlich in elektronischer Form zum Zeitpunkt der Erhebung bereitgestellt werden.

Sofern der Verantwortliche eine Webseite betreibt, kann er die erforderlichen Informationen „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ anbieten.

Bei nicht digitalen Sachverhalten führt jedoch das Erfordernis der Information zum Zeitpunkt der Erhebung gemäß Art. 13 DS-GVO **zu praktischen Zweifelsfragen**.

Bei mündlichen oder telefonischen Kontakten im geschäftlichen Bereich ist es lebensfremd zu erwarten, dass der Verantwortliche umfassende Datenschutzinformationen erteilt. Bei Aufnahme einer Bestellung, der Entgegennahme einer Visitenkarte oder dem Notieren eines Termins wird er keine Rechtsgrundlage für diese Handlungen benennen oder über die zuständige Datenschutzaufsichtsbehörde, Auskunfts-, Beschwerde- und sonstige Betroffenenrechte informieren.

Eine solche Kaskade von Information würde vielfach auf das Unverständnis der Betroffenen stoßen. Mehr Akzeptanz für den Datenschutz im Alltag sieht anders aus.

Wir haben uns in der DSK erfreulicherweise auf einen recht weitgehenden Reformvorschlag verständigt: Die **Informationspflichten** sollen danach **in bestimmten Fällen nur noch auf Verlangen** der betroffenen Person erfüllt werden müssen.

Das gilt vor allem bei einer **Datenverarbeitung**, die der Betroffene **erwarten muss und bei der keine besonderen Risikofaktoren** vorliegen.

Ausnahmen von diesem Grundsatz wären dann etwa die Weitergabe der erhobenen Daten an Dritte, oder die Verarbeitung besonders sensibler Daten nach Art. 9.

Auch beim Profiling muss weiterhin umfassend informiert werden.

Was die Informationspflichten angeht, möchte ich den sogenannten **Mehrebenenansatz („layered approach“)** erwähnen, der vom Europäischen Datenschutzausschuss in seinen Leitlinien zur Transparenz vorgesehen ist. Diese Möglichkeit einer stufenweisen Erfüllung der Informationspflichten über mehrere Ebenen ist zwar in der DSGVO nicht ausdrücklich erwähnt, aber sinnvoll und praxistauglich.

Ist es wirklich ein datenschutzrechtliches Problem, wenn bei einem telefonischen Erstkontakt mit einer betroffenen Person nicht die gesamte Datenschutzerklärung, sondern nur die wichtigsten Informationen zur Verfügung gestellt werden?

Hier dürfte es doch genügen, auf die Abrufbarkeit der gesamten Erklärung im Internet oder eventuell auf eine separat vom Band abrufbare Datenschutzerklärung mit Hinweis auf die Betroffenenrechte zu verweisen.

Auch ein symbolhaftes Hinweisschild bei der Videoüberwachung mit Angabe eines Links zur ausführlichen Datenschutzerklärung fällt unter den Mehrebenenansatz.

1.3 Unabhängigkeit der Aufsichtsbehörden

1. 3.1 Unabhängige nationale Aufsichtsbehörden

Lassen Sie mich abschließend noch kurz die Stellung der Aufsichtsbehörden für den Datenschutz ansprechen.

Sie sind **völlig unabhängig**. Ihre Befugnisse wurden durch die DSGVO und die nationalen Regeln deutlich erweitert.

- **Untersuchungs- und Abhilfebefugnisse**
- **Warnungen**
- **Anweisungen**
- **Anordnung der Aussetzung der Übermittlung**
- **Empfindliche Bußgelder**

Für die meisten Verantwortlichen und die Öffentlichkeit steht die Frage im Mittelpunkt, wie teuer ein Verstoß gegen die Vorschriften des Datenschutzes wird.

Da hat sich mit der DSGVO einiges getan. Geldbußen von bis zu 10.000.000 € oder 20.000.000 € bzw. 2 % oder 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres sind nicht von Pappe.

Ich selbst habe eine große Geldbuße in Höhe von 9,5 Millionen Euro gegen einen Telekommunikationsanbieter verhängt. Das klingt viel. Die Obergrenze des im vorliegenden Fall möglichen Bußgeldrahmens hätte aber bei über 73 Millionen Euro gelegen. Das Unternehmen war aber kooperativ und einsichtig, was den Fehler selbst angeht. Die Geldbuße blieb daher im unteren Bereich.

Leider wird das Bußgeld aber vor Gericht angegriffen. Unterstützt durch so manchen juristischen Kommentar, der mich ratlos zurücklässt. Umsatz sei keine Messgröße, vergangene Fehler könnten nicht mit Bußgeldern belegt werden, technische Schutzmaßnahmen für personenbezogene Daten seien nicht definiert und daher nicht sanktionierbar, Unternehmen könnten überhaupt nicht sanktioniert werden, nur Einzelpersonen.

Gehen wir das mal im Einzelnen durch …

1.3.2 Der EDSA

Auch bei der Datenschutzaufsicht ist der Ansatz der DSGVO ist durch und durch europäischer.

Der Europäische Datenschutzausschuss ist daher ausschlaggebender Bedeutung. Er soll für eine einheitliche Anwendung der Datenschutzvorschriften in der EU sorgen.

Ich bin als Bundesbeauftragter gemeinsamer Vertreter aller deutschen Aufsichtsbehörden.

Kernaufgabe des EDSA ist **die einheitliche Anwendung der DSGVO und der** EU-Datenschutz-Richtlinie 2016/68 für den Bereich Justiz und Inneres **(JI-Richtlinie).**

Außerdem kann der EDSA Leitlinien, Empfehlungen und bewährte Verfahren zur Auslegung der DSGVO und der JI-Richtlinie erlassen.

Üblicherweise treffen wir uns monatlich im Plenum und in zahlreichen Arbeitsgruppen. Meine Behörde ist in allen Arbeitsgruppen vertreten, zum Teil federführend.

Die Corona- Krise führt aber natürlich auch hier zu Einschränkungen, so dass wir auch die europäische Gremienarbeit in den letzten Monaten auf Video- und Telefonkonferenzen umstellen mussten. Diese finden mittlerweile mindestens wöchentlich statt. Sie sehen also, dass uns auch die Krise nicht daran hindert uns regelmäßig über die wichtigen datenschutzrechtlichen Fragen auszutauschen.

Wie wichtig die „normale“ Fortführung des EDSA-Betriebs ist, zeigt ein Blick auf seinen bisherigen Output: Neben allgemeinen Leitlinien zur Auslegung der DSGVO wurden seit Ende 2018 zahlreiche Stellungnahmen im Kohärenzverfahren nach Art. 64 DSGVO verabschiedet.

Hauptgegenstand waren Entwürfe von Listen der nationalen Aufsichtsbehörden zu Datenverarbeitungen, für die nach Art. 35 Abs. 4 DSGVO Datenschutzfolgenabschätzungen erforderlich sind. Im Kohärenzverfahren sollen die nationalen Listen angeglichen werden.

Mit Stand Januar 2020 hat der EDSA 50 Stellungnahmen im Rahmen des Kohärenzverfahrens nach Art. 64 DSGVO angenommen.

Ärgerlich ist jedoch, dass noch über keine der datenschutzrechtlich problematischen Verhaltensweisen der großen internationalen Datenkonzerne entschieden werden konnte.

Das liegt daran, dass die federführenden Aufsichtsbehörden aus Irland und Luxemburg noch keinen Beschlussentwurf vorgelegt haben.

Hier liegt die Achillesferse der DSGVO. Gelingt es in absehbarer Zeit nicht, die bereits seit zwei Jahren anhängigen Verfahren gegen Facebook, Amazon und Co auf nationaler Ebene und sodann im Rahmen der EDSA-Beratungen abzuschließen, stehen Reputation und Akzeptanz des gesamten Regelwerks auf dem Spiel.

Den EDSA selbst trifft keine Schuld.

Er hat keine formellen Möglichkeiten, das Arbeitstempo der im konkreten Fall federführend zuständigen nationalen Aufsichtsbehörde – sei es aufgrund mangelnder Ressourcen, eines komplizierten nationalen Verfahrensrechts oder sonstigen (Beweg-)Gründen – zu beschleunigen. Er hat nach der DSGVO lediglich die Aufgabe, Meinungsverschiedenheiten zwischen den Aufsichtsbehörden in grenzüberschreitenden Verfahren zu schlichten.

Von Tag zu Tag zweifele ich mehr daran, ob dieses System unverändert bleiben kann oder einer grundlegenden Reform bedarf. Ich habe der irischen Behörde angeboten, Arbeiten in einzelnen Fällen zu übernehmen und hierfür ein gangbares Verfahrenskonzept vorgelegt. Die Reaktion darauf war und ist … verhalten.

Immer mehr spricht daher für eine europäische Datenschutzbehörde, die besonders wichtige Verfahren bei z.B. einer ¾-Mehrheit im EDPB übernehmen kann und für die ein zu schaffendes europäisches Verwaltungsrecht besteht, das den Datenschutz nicht aushebelt, sondern schnell zu Ergebnissen führt.

III.Schlussbemerkung

Ich möchte Sie zum Abschluss um zwei Dinge bitten.

Schützen Sie die DSGVO vor der Abrissbirne derer, denen Datenschutz schon immer ein Dorn im Auge war und die jetzt in der Krise versuchen, den Schutz der Menschen in einer zunehmend digitalisierten Welt beiseite zu räumen.

Unterstützen sie die fundierten Vorschläge der DSK für eine behutsame und nachhaltige Weiterentwicklung der DSGVO.

Weisen sie bitte auch die vielen Angriffe auf das neue europäische Gesetzeswerk energisch zurück. Werweisen Sie dabei als Datenschützerinnen und Datenschützer mit Selbstbewusstsein auf die nationalen und internationalen Erfolge des neuen europäischen Rechs. Das hat den Sturm der Pandemie überstanden und wird auch kommende Herausforderungen meistern.

Ich danke Ihnen für Ihre Aufmerksamkeit und hoffe sehr, beim nächsten Mal wieder direkt mit Ihnen sprechen zu können.